HIRSCHMANN
A BELDEN BRAND

Reference Manual

Web-based Interface
Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100, MACH 1000, MACH 4000

Industrial ETHERNET (Gigabit) Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100, MACH 1000, MACH 4000

Technical Support
HAC.Support@Belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2010Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use. For devices with embedded software, the end-user license agreement on the enclosed CD applies.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann-ac.de).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Contents

About this Manual 7

Key 9

Opening the Web-based Interface 11

1 Basic Settings 15

1.1 System 16

1.2 Network 22

1.3 Software 24
1.3.1 View the software versions present on the device 24
1.3.2 TFTP Software Update 25
1.3.3 HTTP Software Update 25
1.3.4 Automatic software update by ACA 26

1.4 Port Configuration 27

1.5 Power over ETHERNET 29

1.6 Loading/Saving the Configuration 32
1.6.1 Loading the configuration 33
1.6.2 Saving the Configuration 33
1.6.3 URL 34
1.6.4 Deleting a configuration 34
1.6.5 Using the AutoConfiguration Adapter (ACA) 35
1.6.6 Canceling a configuration change 37

1.7 Restart 38

2 Security 41

2.1 Password / SNMPv3 access 42

2.2 SNMPv1/v2 Access Settings 45

2.3 Telnet/Web/SSH Access 48
2.3.1 Description of Telnet Access 49
2.3.2 Description of Web Access 49
2.3.3 Description of SSH Access 50

2.4 Restricted Management Access 51

2.5 Port Security 54

2.6 IEEE 802.1X Port Authentication 57
2.6.1 IEEE 802.1X Global 57
2.6.2 IEEE 802.1X Port Configuration 59
2.6.3 IEEE 802.1X Port Statistics 62
2.6.4 RADIUS Server Settings for IEEE 802.1X 64

3 Time 67

3.1 SNTP configuration 69

3.2 PTP (IEEE 1588) 73
3.2.1 PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 74
3.2.2 PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 78
3.2.3 PTP Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 80
3.2.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE) 85

4 Switching 89

4.1 Switching Global 90

4.2 Filters for MAC addresses 94

4.3 Rate Limiter 96
4.3.1 Rate Limiter settings for RS20/RS30/40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS 97
4.3.2 Rate Limiter Settings (PowerMICE and MACH 4000) 99

4.4 Multicasts 100
4.4.1 IGMP (Internet Group Management Protocol) 100
4.4.2 GMRP (GARP Multicast Registration Protocol) 107

4.5 VLAN 110
4.5.1 VLAN Global 110
4.5.2 Current VLAN 113
4.5.3 VLAN Static 115
4.5.4 VLAN Port 117

5 QoS/Priority 121

5.1 Global 122

5.2 Port Configuration 125
5.2.1 Entering the port priority 127

5.2.2 Selecting the trust mode (PowerMICE, MACH 104, MACH 1040 and MACH 4000) 128
5.2.3 Displaying the untrusted traffic class (PowerMICE, MACH 104, MACH 1040 and MACH 4000) 129
5.3 802.1D/p mapping 130
5.4 IP DSCP mapping 132

6 Redundancy 135

6.1 Link Aggregation 136
6.2 Ring Redundancy 139
6.2.1 Configuring the HIPER-Ring 141
6.2.2 Configuring the MRP-Ring 145
6.2.3 Configuring the Fast HIPER-Ring(RSR20, RSR30, MACH 1000) 148
6.3 Sub-Ring 151
6.3.1 Sub-Ring configuration 152
6.3.2 Sub-Ring - New Entry 155
6.4 Ring/Network Coupling 157
6.4.1 Preparing a Ring/Network coupling 157
6.5 Spanning Tree 164
6.5.1 Global 166
6.5.2 MSTP (Multiple Spanning Tree) 173
6.5.3 Port 179

7 Advanced 189

7.1 DHCP Relay Agent 190
7.2 DHCP Server 192
7.2.1 Global 192
7.2.2 Pool 194
7.2.3 Lease Table 198
7.3 Industrial Protocols 200
7.3.1 PROFINET IO 200
7.3.2 EtherNet/IP 202
7.4 Command Line 203

8 Diagnostics 205

8.1 Syslog 206

8.2 Event Log 211

8.3 Ports 212
8.3.1 Statistics table 212
8.3.2 Utilization 213
8.3.3 SFP modules 215
8.3.4 TP Cable Diagnosis 216

8.4 Configuration Check 218

8.5 Topology Discovery 220

8.6 Port Mirroring 222

8.7 Device Status 224

8.8 Signal contact 227
8.8.1 Manual setting 227
8.8.2 Function monitoring 227
8.8.3 Device status 229
8.8.4 Configuring traps 229

8.9 Alarms (Traps) 231

8.10 Report 234

8.11 IP address conflict detection 236

8.12 Self Test 238

8.13 Service mode 239
8.13.1 Activating the service mode 240
8.13.2 Deactivating the service mode 241

A Appendix 243

B Readers' Comments 251

C Index 253

D Further Support 257

About this Manual

The "Web-based Interface" reference manual contains detailed information on using the Web interface to operate the individual functions of the device.

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Industry Protocols” user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP or PROFINET IO.

The Network Management Software HiVision/Industrial HiVision provides you with additional options for smooth configuration and monitoring:

- Configuration of multiple devices simultaneously.
- Graphical interface with network layouts.
- Auto-topology discovery.
- Event log.
- Event handling.
- Client / Server structure.
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway

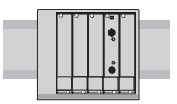
Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Indicates a cross-reference with a stored link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

Opening the Web-based Interface

To open the Web-based interface, you need a Web browser (a program that can read hypertext), for example Mozilla Firefox version 1 or later, or Microsoft Internet Explorer version 6 or later.

Note: The Web-based interface uses Java software 6 (“Java™ Runtime Environment Version 1.6.x”).

Install the software from the enclosed CD-ROM. To do this, you go to “Additional Software”, select `Java Runtime Environment` and click on “Installation”.

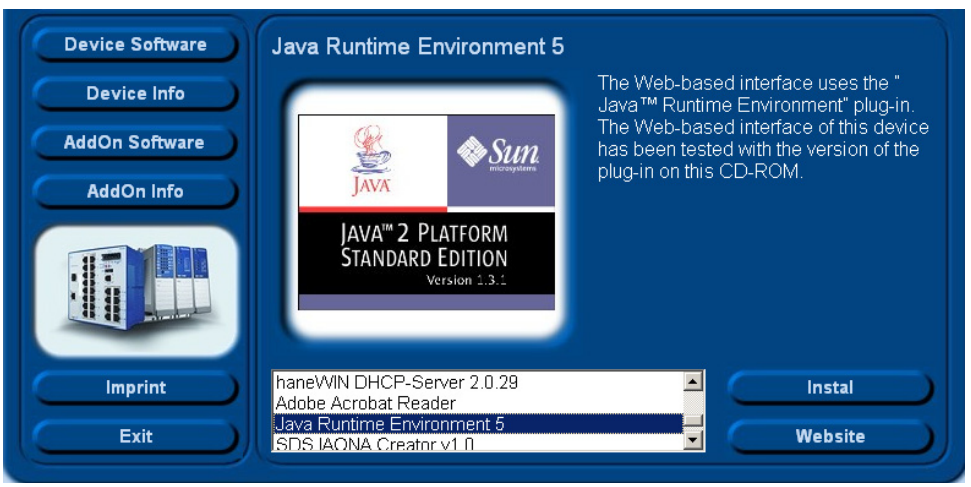

Device Software
Device Info
AddOn Software
AddOn Info
Imprint
Exit
Java Runtime Environment 5
The Web-based interface uses the " Java™ Runtime Environment" plug-in. The Web-based interface of this device has been tested with the version of the plug-in on this CD-ROM.
JAVA™ 2 PLATFORM STANDARD EDITION
haneWIN DHCP-Server 2.0.29
Adobe Acrobat Reader
Java Runtime Environment 5
Instal
Website

Figure 1: Installing Java

☐ Start your Web browser.
☐ Check that you have activated JavaScript and Java in your browser settings.
☐ Establish the connection by entering the IP address of the device which you want to administer via the Web-based management in the address field of the Web browser. Enter the address in the following form:
`http://xxx.xxx.xxx.xxx`

The login window appears on the screen.

Figure 2: Login window

☐ Select the desired language.
☐ In the drop-down menu "Login", you select
– user, to have read access, or
– admin, to have read and write access
to the device.
☐ The password “public”, with which you have read access for the login "user", is preset in the password field. If you wish to have write access to the device, use the login "admin", select the contents of the password field and overwrite it with the password “private” (default setting).
☐ Click on OK.

The Web site of the device appears on the screen.

Note: The changes you make in the dialogs will be copied to the device when you click “Set”. Click “Reload” to update the display.
To save any changes made so that they will be retained after a power cycle or reboot of the device use the save option on the "Load/Save" dialog (see on page 32 “Loading/Saving the Configuration“)

Note: You can block your access to the device by entering an incorrect configuration.
Activating the function “Cancel configuration change” in the “Load/Save” dialog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the device.

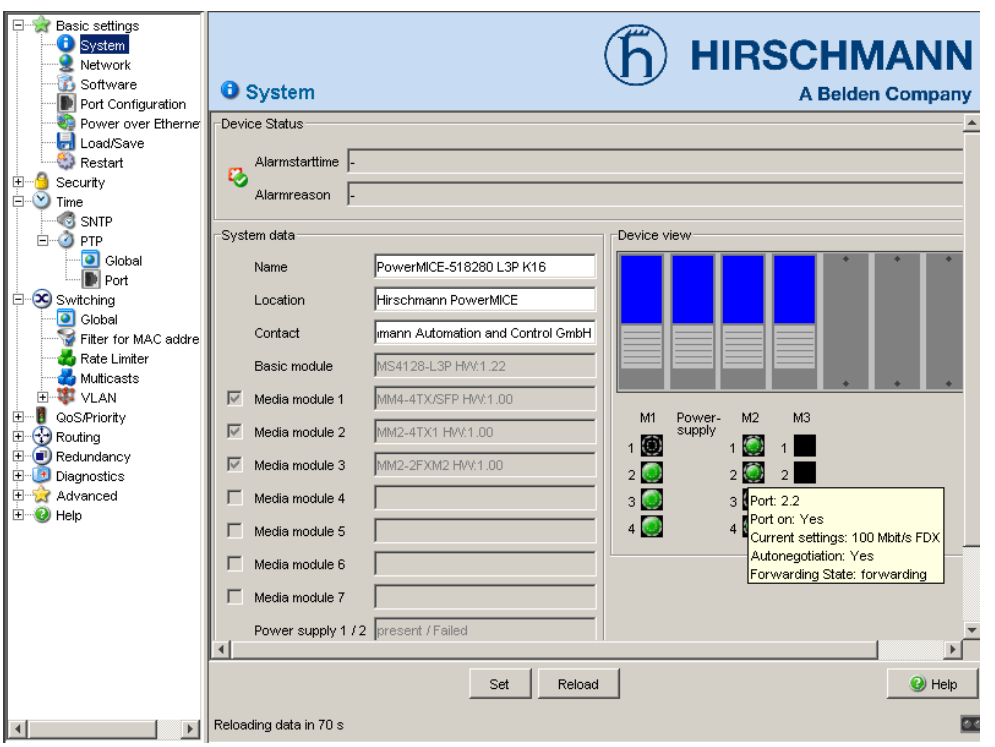
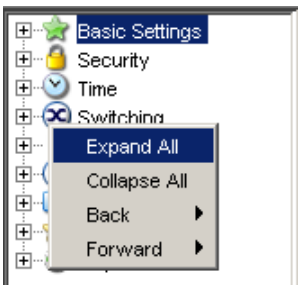


Figure 3: Website of the device with speech-bubble help

The menu section displays the menu items. By placing the mouse pointer in the menu section and clicking the alternate mouse button you can use “Back” to return to a menu item you have already selected, or “Forward” to jump to a menu item you have already selected.



1 Basic Settings

The Basic Settings menu contains the dialogs, displays and tables for the basic configuration:

- System
- Network
- Software
- Port configuration
- Power over Ethernet
- Load/Save
- Restart

1.1 System

The “System“ submenu in the basic settings menu is structured as follows:

- Device Status
- System data
- Device view
- Reloading data

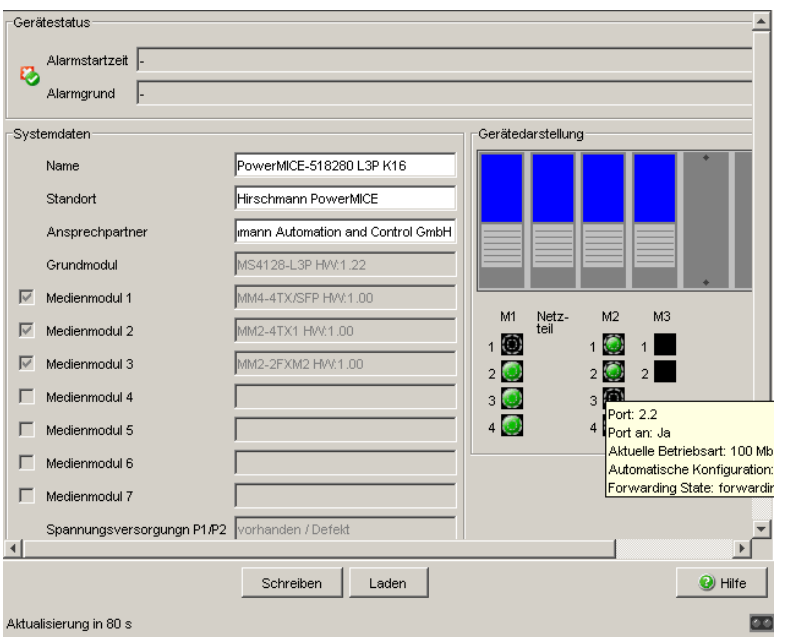


Figure 4: "System" Submenu

Device Status

This section of the website provides information on the device status and the alarm states the device has detected.

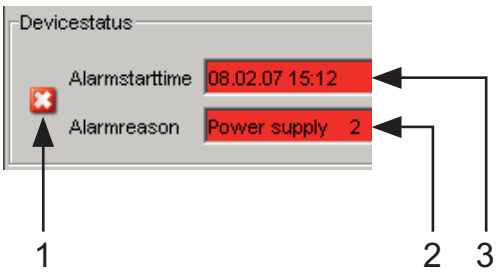


Figure 5: Device status and display of detected alarms
1 - Symbol indicates the Device Status
2 - Cause of the oldest existing alarm detected
3 - Time of the oldest existing alarm detected

System Data

This area of the website displays the system parameters of the device. Here you can change

- the system name,
- the location description,
- the name of the contact person for this device,
- the availability of the media modules (see fig. 6)
- the temperature threshold values.

Name	Meaning
Name	System name of this device
Location	Location of this device
Contact	The contact for this device
Basic module	Hardware version of the device
Media module 1	Hardware version of media module 1
Media module 2	Hardware version of media module 2
Media module 3	Hardware version of media module 3
Media module 4	Hardware version of media module 4
Media module 5	Hardware version of media module 5
Media module 6	Hardware version of media module 6
Media module 7	Hardware version of media module 7
Power supply (P1/P2)	Status of power units (P1/P2)
Power supply 3-1/3-2	Status of power units 3-1/3-2
Power supply 4-1/4-2	Status of power units 4-1/4-2
Fan	Status of fans

Table 1: System Data

Uptime	Time that has elapsed since this device was last restarted.
Temperature	Temperature of the device. Lower/upper temperature threshold values. If the temperature goes outside this range, the device generates an alarm.

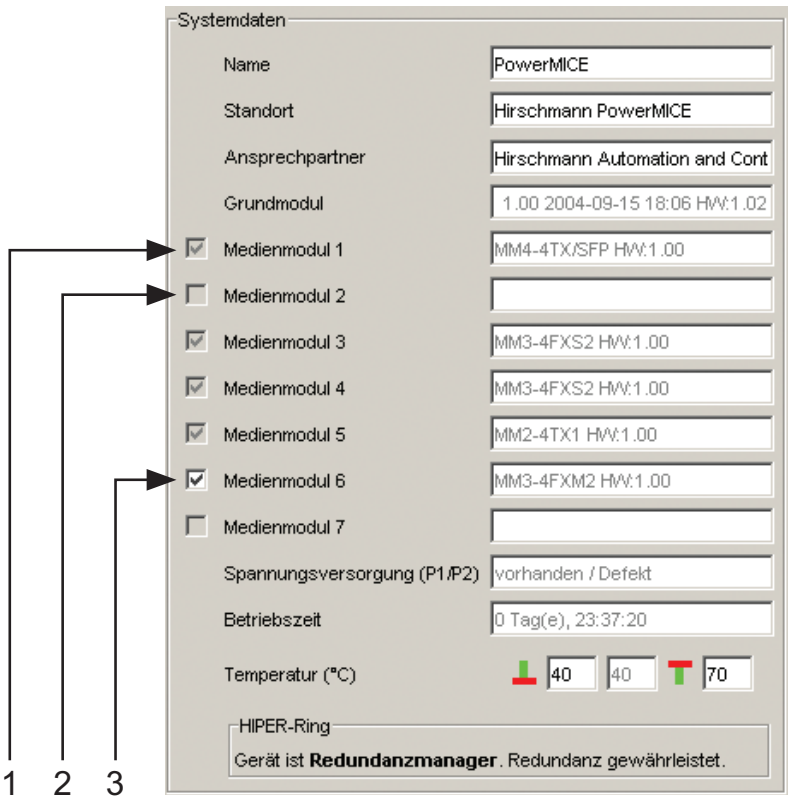


Figure 6: Availability of the media modules
1 - Module present
2 - Empty slot
3 - Module was removed. Click this check mark to define this slot as an empty slot.

Device View

The device view shows the device with the current configuration. The symbols underneath the device view represent the status of the individual ports.

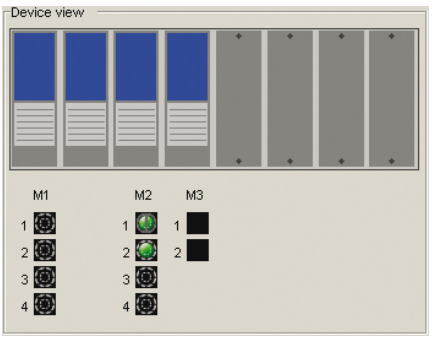


Figure 7: Device View

Meaning of the symbols:

The port (10, 100 Mbit/s, 1, 10 Gbit/s) is enabled and the connection is OK.

The port is disabled by the management and it has a connection.

The port is disabled by the management and it has no connection.

The port is in autonegotiation mode.

The port is in HDX mode.

The port is in RSTP discarding mode (100 Mbit/s).

The port is in routing mode (100 Mbit/s).

Updating

This area of the website at the bottom left displays the countdown time until the applet requests the current data of this dialog again. Clicking the "Reload" button calls the current dialog information immediately.
The applet polls the current data of the device automatically every 100 seconds.

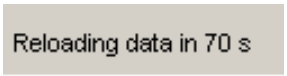


Figure 8: Time until update

1.2 Network

With the `Basic settings:Network` dialog you define the source from which the device gets its IP parameters after starting, and you assign the IP parameters and VLAN ID and configure the HiDiscovery access.

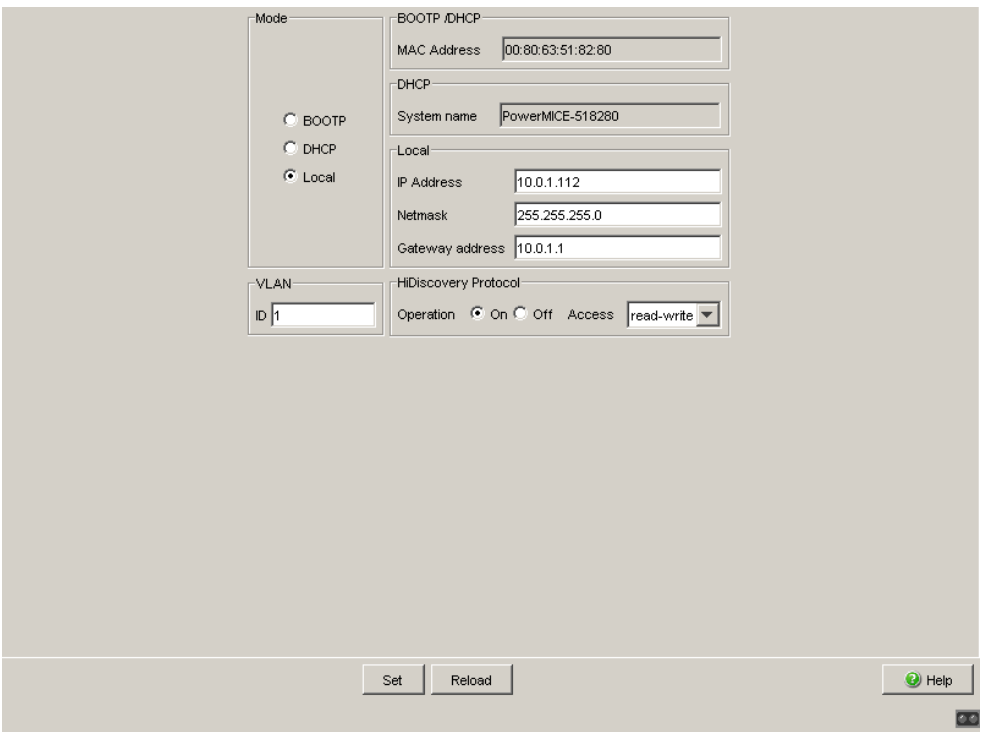


Figure 9: Network parameters dialog

☐ Under “Mode”, you enter where the device gets its IP parameters:
- In the BOOTP mode, the configuration is via a BOOTP or DHCP server on the basis of the MAC address of the device (see on page 32 “Loading/Saving the Configuration“).
- In the DHCP mode, the configuration is via a DHCP server on the basis of the MAC address or the name of the device (see on page 32 “Loading/Saving the Configuration“).
- In the local mode the network parameters in the device memory are used.

☐ Enter the parameters on the right according to the selected mode.

☐ You enter the name applicable to the DHCP protocol in the “Name” line in the system dialog of the Web-based interface.

☐ The “VLAN” frame enables you to assign a VLAN to the agent. If you enter 0 here as the VLAN ID (not included in the VLAN standard version), the agent will then be accessible from all VLANs.

☐ The HiDiscovery protocol allows you to allocate an IP address to the device on the basis of its MAC address. Activate the HiDiscovery protocol if you want to allocate an IP address to the device from your PC with the enclosed HiDiscovery software (state on delivery: operation “on”, access “read-write”).

1.3 Software

The software dialog enables you display the software versions in the device and to carry out a software update of the device via file selection, tftp or ACA.

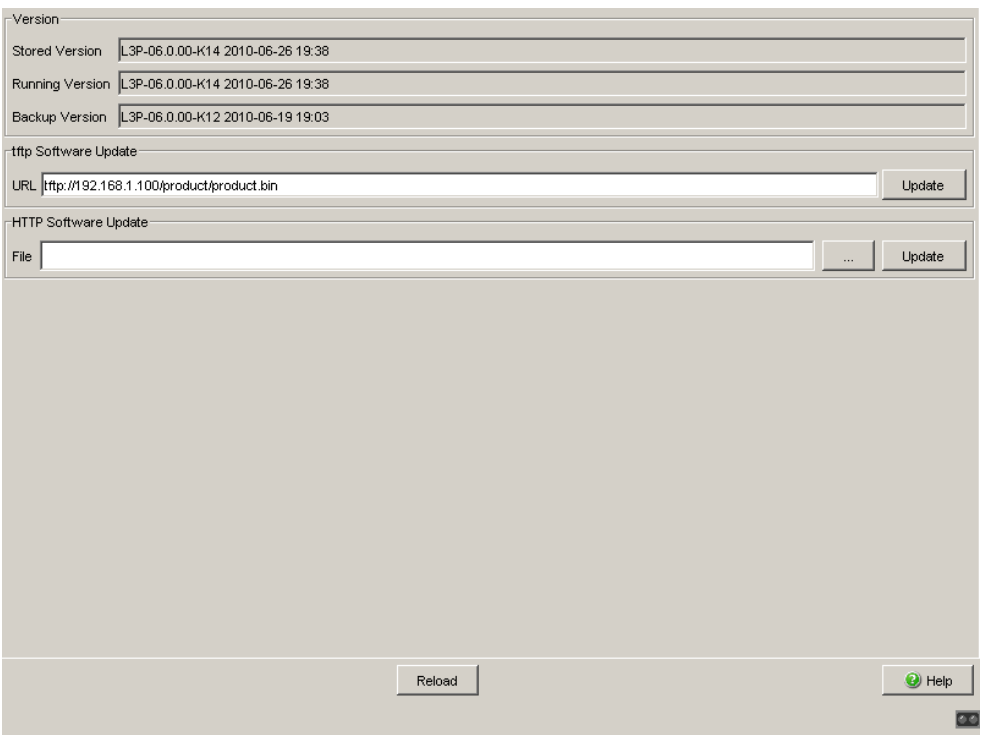


Figure 10: Software dialog

1.3.1 View the software versions present on the device

You can view:

- Stored Version
  The software version stored in the flash memory.

- Running Version
  The currently loaded software version.
- Backup Version
  The previous software version stored in the flash memory.

1.3.2 TFTP Software Update

For a tftp update you need a tftp server on which the software to be loaded is stored.
The URL identifies the path to the software stored on the tftp server. The URL is in the format
tftp://IP address of the tftp server/path name/file name
(e.g. `tftp://192.168.1.1/device/device.bin`).
Click "tftp Update" to load the software from the tftp server to the device.
To start the new software after loading, cold start the device (see on page 38 “Restart“).

1.3.3 HTTP Software Update

For an HTTP software update (via a file selection window), the device software must be on a data carrier that you can access via a file selection window from your workstation.

☐ In the file selection frame, click on “...”.
☐ In the file selection window, select the device software (name type: *.bin, e.g. device.bin) and click on “Open”.
☐ Click on “Update” to transfer the software to the device.

The end of the update is indicated by one of the following messages:

- Update completed successfully.
- Update failed. Reason: incorrect file.
- Update failed. Reason: error when saving.

- File not found (reason: file name not found or does not exist).
- Connection error (reason: path without file name).

☐ After the update is completed successfully, you activate the new software: Select the `Basic settings: Restart` dialog and perform a cold start. In a cold start, the device reloads the software from the non-volatile memory, restarts, and performs a self-test.

☐ In your browser, click on “Reload” so that you can access the device again after it is booted.

1.3.4 Automatic software update by ACA

The device also allows you to perform an automatic software update using the ACA. You will find the relevant details in the document “Basic Configuration User”, chapter “Automatic Software Update by ACA”.

1.4 Port Configuration

This configuration table allows you to configure each port of the device and also display each port‘s current mode of operation (link state, bit rate (speed) and duplex mode).

- In the “Name” column, you can enter a name for every port.
- In the “Ports on” column, you can switch on the port by selecting it here.
- In the “Propagate connection error” column, you can specify that a link alarm will be forwarded to the device status and/or the the signal contact is to be opened.
- In the “Automatic Configuration” column, you can activate the automatic selection of the the operating mode (Autonegotiation) and the automatic assigning of the connections (Auto cable crossing) of a TP port by selecting the appropriate field. After the autonegotiation has been switched on, it takes a few seconds for the operating mode to be set.
- In the “Manual Configuration” column, you set the operating mode for this port. The choice of operating modes depends on the media module. The possible operating modes are:
  - 10 Mbit/s half duplex (HDX),
  - 10 Mbit/s full duplex (FDX),
  - 100 Mbit/s half duplex (HDX),
  - 100 Mbit/s full duplex (FDX),
  - 1000 Mbit/s half duplex (HDX),
  - 1000 Mbit/s full duplex (FDX) and
  - 10 Gbit/s full duplex (FDX).
- The “Link/Current Operating Mode” column displays the current operating mode and thereby also an existing connection.
- In the “Cable Crossing (Auto. Conf. off)” column, you assign the connections of a TP port, if “Automatic Configuration” is deactivated for this port. The possible settings are:
  - enable: the device swaps the send and receive line pairs of the TP cable for this port (MDIX).
  - disable: the device does not swap the send and receive line pairs of the TP cable for this port (MDI).
  - unsupported: the port does not support this function (optical port, TP SFP port).
- In the “Flow Control” column, you checkmark this port to specify that flow control is active here. You also activate the global “Flow Control” switch (see on page 90 “Switching Global“).

Note: The active automatic configuration has priority over the manual configuration.

Note: If you are using link aggregation, pay attention to its configuration (see on page 136 “Link Aggregation“).

Note: When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports.
If the flow control and the redundancy function are active at the same time, there is a risk of the redundancy failing.

Note: The following settings are required for the ring ports in a HIPER-Ring:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

Table 2: Port Settings for Ring Ports

When you switch the DIP switch for the ring ports, the device sets the required settings for the ring ports in the configuration table. The port, which has been switched from a ring port to a normal port, is given the settings Autonegotiation (automatic configuration) on and Port on. The settings remain changeable for all ports.

1.5 Power over ETHERNET

Devices with Power over ETHERNET (PoE) media modules or PoE ports enable you to supply current to terminal devices such as IP phones via the twisted-pair cable. PoE media modules and PoE ports support Power over ETHERNET according to IEEE 802.3af.
On delivery, the Power over ETHERNET function is activated globally and at all ports.

Nominal power for MS20/30, MACH 1000 and PowerMICE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the PoE media module gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 60 Watt per PoE media module for now.

Nominal power for OCTOPUS 8M-PoE:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Because the device gets its PoE voltage externally, the device does not know the possible nominal power.
The device therefore assumes a “nominal power” of 15 Watt per PoE port for now.

Nominal power for MACH 4000:
The device provides the nominal power for the sum of all PoE ports plus a surplus. Should the connected devices require more PoE power than is provided, the device then switches PoE off at the ports. Initially, the device switches PoE off at the ports with the lowest PoE priority. If multiple ports have the same priority, the device first switches PoE off at the ports with the higher port number.

- ☐ With “Function on/off” you turn the PoE on or off.
- ☐ With “Send Trap” you can get the device to send a trap in the following cases:
  - – If a value exceeds/falls below the performance threshold.
  - – If the PoE supply voltage is switched on/off at at least one port.
- ☐ Enter the power threshold in “Threshold”. When this value is exceeded/ not achieved, the device will send a trap, provided that “Send trap” is enabled. For the power threshold you enter the power yielded as a percentage of the nominal power.

- ☐ “Nominal Power” displays the power that the device nominally provides for all PoE ports together.
- ☐ “Reserved Power” displays the maximum power that the device provides to all the connected PoE devices together on the basis of their classification.
- ☐ “Delivered Power” shows how large the current power requirement is at all PoE ports.

The difference between the "nominal" and "reserved" power indicates how much power is still available to the free PoE ports.

- ☐ In the “POE on” column, you can enable/disable PoE at this port.
- ☐ The “Status” column indicates the PoE status of the port.
- ☐ In the “Priority” column (MACH 4000), set the PoE priority of the port to “low”, “high” or “critical”.
- ☐ The “Class” column shows the class of the connected device:
  ClassMaximum power delivered
  0: 15.4 W = state on delivery
  1: 4.0 W
  2: 7.0 W
  3: 15.4 W
  4: Reserved, treat as class 0
- ☐ The “Name” column indicates the name of the port, see `Basic settings:Port configuration`.

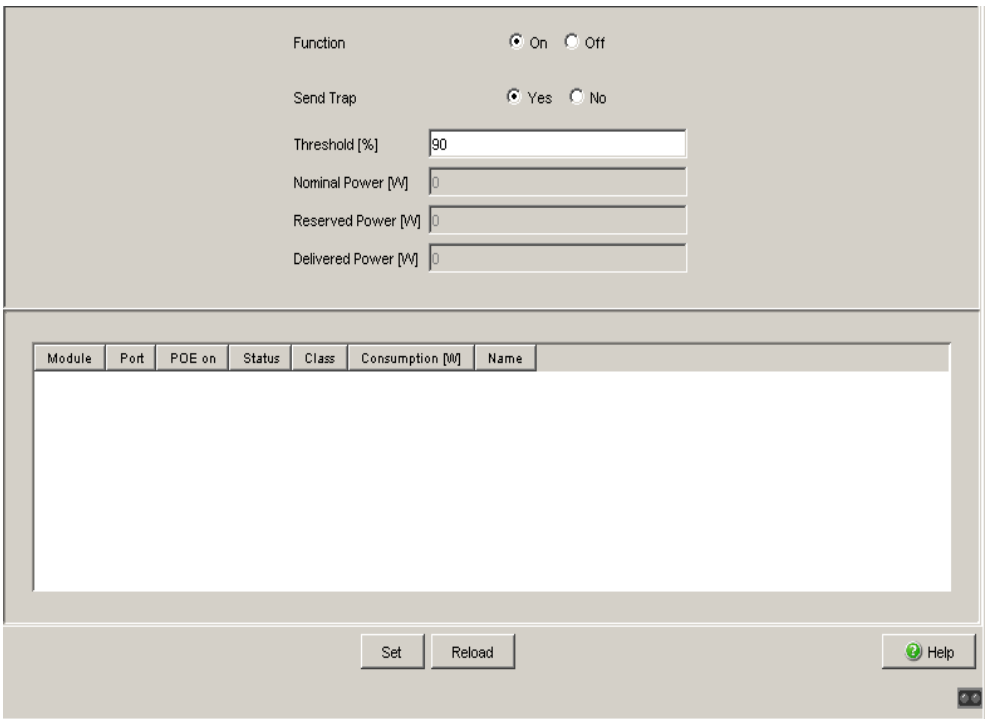


Figure 11: Power over Ethernet dialog

1.6 Loading/Saving the Configuration

With this dialog you can:

- load a configuration,
- save a configuration,
- enter a URL,
- restore the delivery configuration,
- use the ACA for configuring,
- cancel a configuration change.

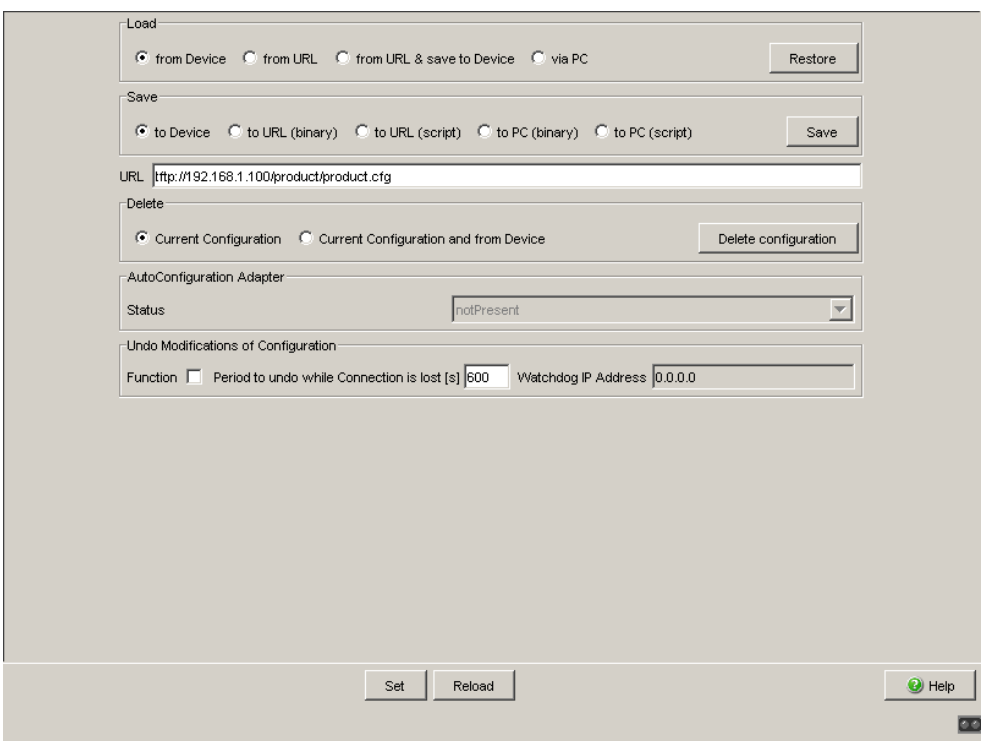


Figure 12: Load/Save dialog

1.6.1 Loading the configuration

In the “Load” frame, you have the option to

- load a configuration saved on the device,
- load a configuration stored under the specified URL,
- load a configuration stored on the specified URL and save it on the device,
- load a configuration stored on the PC as an editable and readable script or in binary form,

If you change the current configuration (for example, by switching a port off), the Web-based interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the Web-based interface displays the “load/save” symbol as a disk again.

1.6.2 Saving the Configuration

In the “Save” frame, you have the option to

- save the current configuration on the device,
- save the current configuration in binary form in a file under the specified URL, or as an editable and readable script,
- save the current configuration in binary form or as an editable and readable script on the PC.

Note: The loading process started by DHCP/BOOTP (see “Network“ on page 22) shows the selection of “from URL & save local” in the “Load” frame. If you get an error message when saving a configuration, this could be due to an active loading process. DHCP/BOOTP only finishes a loading process when a valid configuration has been loaded. If DHCP/BOOTP does not find a valid configuration, finish the loading process by loading the local configuration in the “Load” frame.

If you change the current configuration (for example, by switching a port off), the Web-based interface changes the “load/save” symbol in the navigation tree from a disk symbol to a yellow triangle. After saving the configuration, the Web-based interface displays the “load/save” symbol as a disk again.

After you have successfully saved the configuration on the device, the device sends an alarm (trap) `hmConfigurationSavedTrap` together with the information about the AutoConfiguration Adapter (ACA), if one is connected. When you change the configuration for the first time after saving it, the device sends a trap `hmConfigurationChangedTrap`.

1.6.3 URL

The URL identifies the path to the tftp server on which the configuration file is to be stored. The URL is in the format: tftp://IP address of the tftp server/ path name/file name (e.g. `tftp://192.168.1.100/device/config.dat`).

Note: The configuration file includes all configuration data, including the passwords for accessing the device. Therefore pay attention to the access rights on the tftp server.

1.6.4 Deleting a configuration

In the "Delete" frame, you have the option to

- Reset the current configuration to the state on delivery. The configuration saved on the device is retained.

- Reset the device to the state on delivery. After the next restart, the IP address is also in the state on delivery.

1.6.5 Using the AutoConfiguration Adapter (ACA)

The ACAs are devices for saving the configuration data of a device. In the case of a device failure, an ACA enables the configuration data to be transferred easily by means of a substitute device of the same type.

Note: If you replace a device with DIP switches, please ensure that the DIP switch settings are identical.

- **Storing the current configuration data in the ACA:**
  You have the option of transferring the current device configuration, including the SNMP password, on the ACA and the flash memory in the “Save” frame using the “to Switch / Save configuration” option.

  Note: The device saves the configuration, with the exception of its SSH key (see on page 48 “Telnet/Web/SSH Access“). You will find instructions on how to transfer the SSH key of the old device to the new one in the document “Basic Configuration User Manual”, chapter “Replacing defective devices”.

- **Transferring the configuration data from the ACA:**
  When you restart with the ACA connected, the device adopts the configuration data of the ACA and saves it permanently in the flash memory. If the connected ACA does not contain any valid data, for example, if the delivery state is unchanged, the device loads the data from the flash memory.

Note: Before loading the configuration data from the ACA, the device compares the password in the device with the password in the ACA configuration data.

The device loads the configuration data if
- the admin password matches or
- there is no password saved locally or
- the local password is the original default password or
- no configuration is saved locally.

Status	Meaning
notPresent	No ACA present
ok	The configuration data from the ACA and the device match.
removed	The ACA was removed after booting.
notInSync	- The configuration data of the ACA and the device do not match or only one file exists[a], or - no configuration file is present on the ACA or on the device[b].
outOfMemory	The local configuration data is too extensive to be stored on the ACA.
wrongMachine	The configuration data in the ACA originates from a different device type and cannot be read or converted.
checksumErr	The configuration data is damaged.

Table 3: ACA Status

a. In these cases, the ACA status is identical to the status “ACA not in sync”, which sends “Not OK” to the signal contacts, and the device status.
b. In this case, the ACA status (“notInSync”) deviates from the status “ACA not in sync”, which sends “OK” to the signal contacts, and the device status.

1.6.6 Canceling a configuration change

Function

If the function is activated and the connection to the device is interrupted for longer than the time specified in the field “Period to undo while connection is lost [s]”, the device then loads the last configuration saved.

☐ Activate the function before you configure the device so that you will then be reconnected if an incorrect configuration interrupts your connection to the device.

☐ Enter the “Period to undo while the connection is lost [s]” in seconds.
Possible values: 10-600 seconds.
Default setting: 600 seconds.

Note: Deactivate the function after you have successfully saved the configuration. In this way you prevent the device from reloading the configuration after you close the web interface.

Watchdog IP address

“Watchdog IP address” shows you the IP address of the PC from which you have activated the (watchdog) function. The device monitors the link to the PC with this IP address, checking for interruptions.

1.7 Restart

With this dialog you can:

- initiate a cold start of the device. The device reloads the software from the non-volatile memory, restarts, and performs a self-test.
  In your browser, click on “Reload” so that you can access the device again after it is booted.
- initiate a warm start of the device. In this case the device checks the software in the volatile memory and restarts. If a warm start is not possible, a cold start is automatically performed.
- reset the entries with the status “learned” in the filter table (MAC address table).
- reset the ARP table.
  The device maintains an ARP table internally.
  If, for example, you assign a new IP address to a computer and subsequently have problems setting up a connection to the device, you then reset the ARP table.
- reset the port counters.
- delete the log file.

Note: During the restart, the device temporarily does not transfer any data, and it cannot be accessed via the Web-based interface or other management systems such as HiVision.

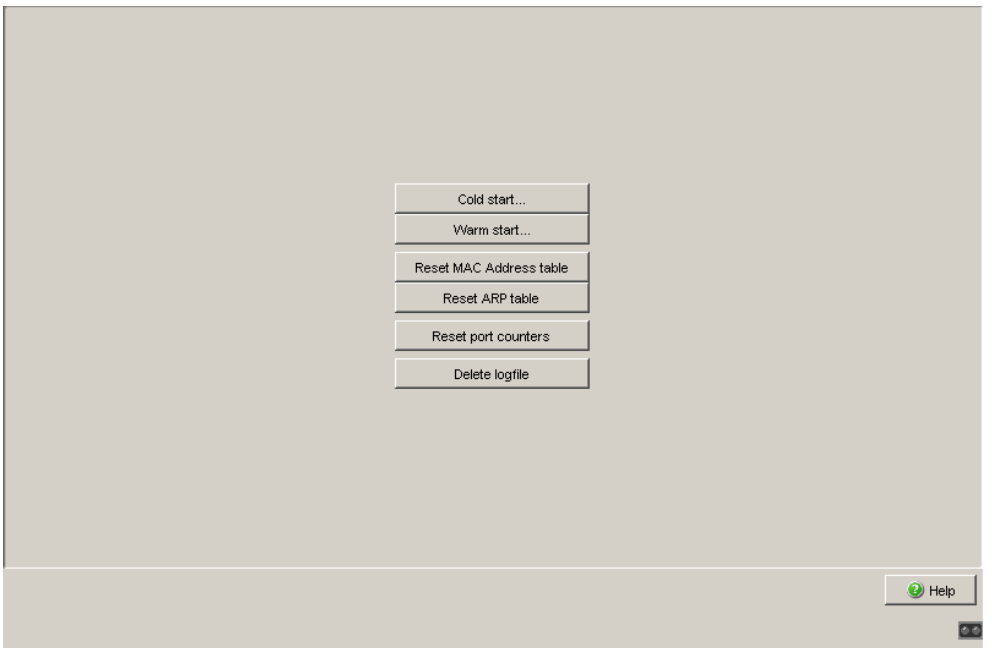


Figure 13: Restart Dialog

2 Security

The “Security” menu contains the dialogs, displays and tables for configuring the security settings:

- Password/SNMPv3 access
- SNMPv1/v2 access
- Telnet/Web/SSH access
- Restricted management access
- Port security
- IEEE 802.1X port authentication

2.1 Password / SNMPv3 access

This dialog gives you the option of changing the read and read/write passwords for access to the device via the Web-based interface, via the CLI, and via SNMPv3 (SNMP version 3). Please note that passwords are case-sensitive.
Set different passwords for the read password and the read/write password so that a user that only has read access (user name “user”) does not know, or cannot guess, the password for read/write access (user name “admin”). If you set identical passwords, when you attempt to write this data the device reports a general error.

The Web-based interface and the user interface (CLI) use the same passwords as SNMPv3 for the users “admin” and “user”.

☐ Select “Modify read-only password (user)” to enter the read password.
☐ Enter the new read password in the “New password” line and repeat your entry in the “Please retype” line.

☐ Select “Modify read-write password (admin)” to enter the read/write password.
☐ Enter the read/write password and repeat your entry.

☐ The “Data encryption” function controls the encryption of the Web-based management data for the transfer between your PC and the device via SNMPv3.
  – When the data encryption is deactivated, the transfer of the configuration data is unencrypted, and is protected from corruption.
  – The Web-based interface always transfers the passwords securely.
  – The Web-based interface always transfers the user name in plain text.
  – The device allows you to set the function differently for the access with the read password and with the read/write password.

Note: When you change the SNMPv3 password for the read/write access, the device automatically synchronizes the readWrite community for the SNMPv1/v2 access to the same value. Similarly, when the read access password is changed, the device synchronizes the readOnly community for SNMPv1/v2 (see on page 45 “SNMPv1/v2 Access Settings“).
As the Web-based interface displays the communities readably in the dialog for SNMPv1/v2, this dialog can only be accessed by a user who has logged in with the user name “admin” and the correct read/write password.

Note: When you change the SNMPv3 password for the user name with which you have logged in to the Web-based interface, log in again so that you can access the Web-based interface of the device again. Otherwise you will get a general error message when you attempt to access it.

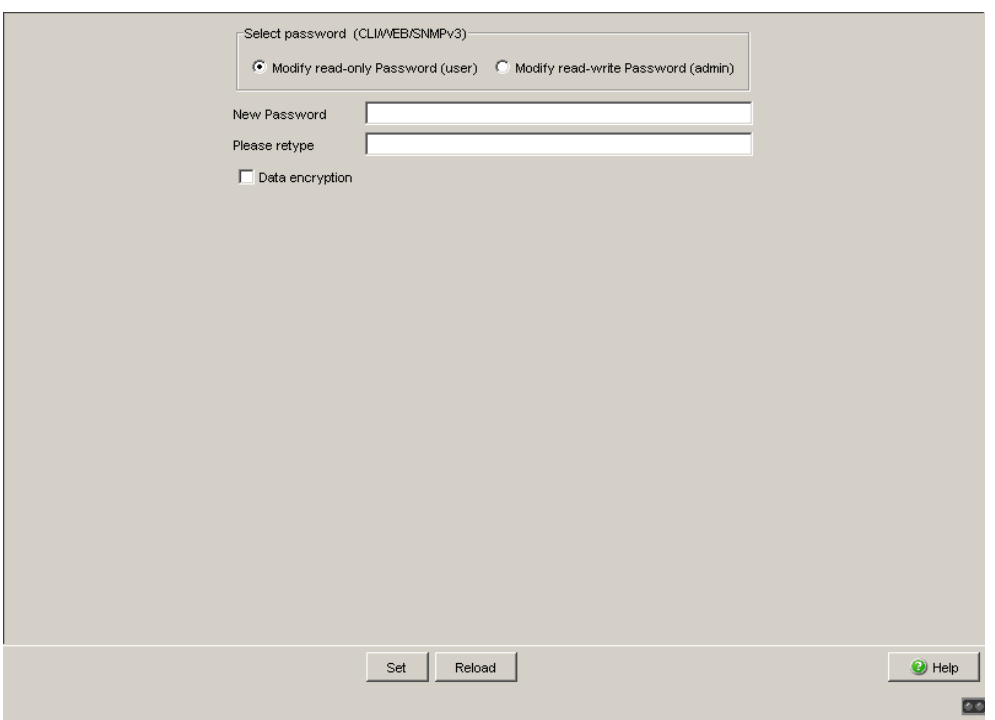


Figure 14: Dialog Password/SNMP Access

Note: If you do not know a password with “read/write” access, you will not have write access to the device.

Note: For security reasons, the device does not display the passwords. Make a note of every change. You cannot access the device without a valid password.

Note: For security reasons, SNMPv3 encrypts the password. With the “SNMPv1” or “SNMPv2” setting in the dialog `Security:SNMPv1/v2 access`, the device transfers the password unencrypted, so that this can also be read.

Note: Use between 5 and 32 characters for the password in SNMPv3, since many applications do not accept shorter passwords.

Access via a Web browser, SSH or Telnet client can be blocked in a separate dialog (see on page 48 “Telnet/Web/SSH Access“).

Access at IP address level is restricted in a separate dialog (see on page 45 “SNMPv1/v2 Access Settings“).

2.2 SNMPv1/v2 Access Settings

With this dialog you can select access via SNMPv1 or SNMPv2. In the state on delivery, both protocols are activated.
You can thus manage the device with HiVision and communicate with earlier versions of SNMP.

Note: To be able to read and/or change the data in this dialog, log in to the Web-based interface with the user name “admin” and the relevant password.

- In the “Index” column, you enter the sequential number to which the access restriction applies.
- In the “Password” column, you enter the password with which a management station may access the device via SNMPv1/v2 from the specified address range. Please note that passwords are case-sensitive.
- In the “IP Address” column, you enter the IP address which may access the device. No entry in this field, or the entry “0.0.0.0”, allows access to this device from computers with any IP address. In this case, the only access protection is the password.
- In the “IP Mask” column, much the same as with netmasks, you have the option of selecting a group of IP addresses.
  Example:
  255.255.255.255: a single IP address
  255.255.255.240 with IP address = 172.168.23.20:
  the IP addresses 172.168.23.16 to 172.168.23.31.

Binary notation of the mask 255.255.255.240:
1111 1111 1111 1111 1111 1111 1111 0000
mask bits
Binary notation of the IP address 172.168.23.20:
1010 1100 1010 1000 0001 0111 0001 0100

The binary representation of the mask with the IP address yields an address range of:
1010 1100 1010 1000 0001 0111 0001 0000 bis
1010 1100 1010 1000 0001 0111 0001 1111
i.e.: 172.168.23.16 to 172.168.23.31

- In the “Access Mode” column, you specify whether this computer can access the device with the read password (access mode “readOnly”) or with the read/write password (access mode “readWrite”).

  Note: The password for the “readOnly” access mode is the same as the SNMPv3 password for read access. The password for the “readWrite” access mode is the same as the SNMPv3 password for read/write access. When you change one of the passwords, the device automatically synchronizes the corresponding password for SNMPv3 (see on page 42 “Password / SNMPv3 access“).

- You can activate/deactivate this table entry in the “Active” column.

  Note: If you have not activated any row, the device does not apply any access restriction with regard to the IP addresses.

- The “Create entry” button enables you to create a new row in the table.
- With “Delete entry” you delete selected rows in the table.

Note: The row with the password currently in use cannot be deleted or changed.

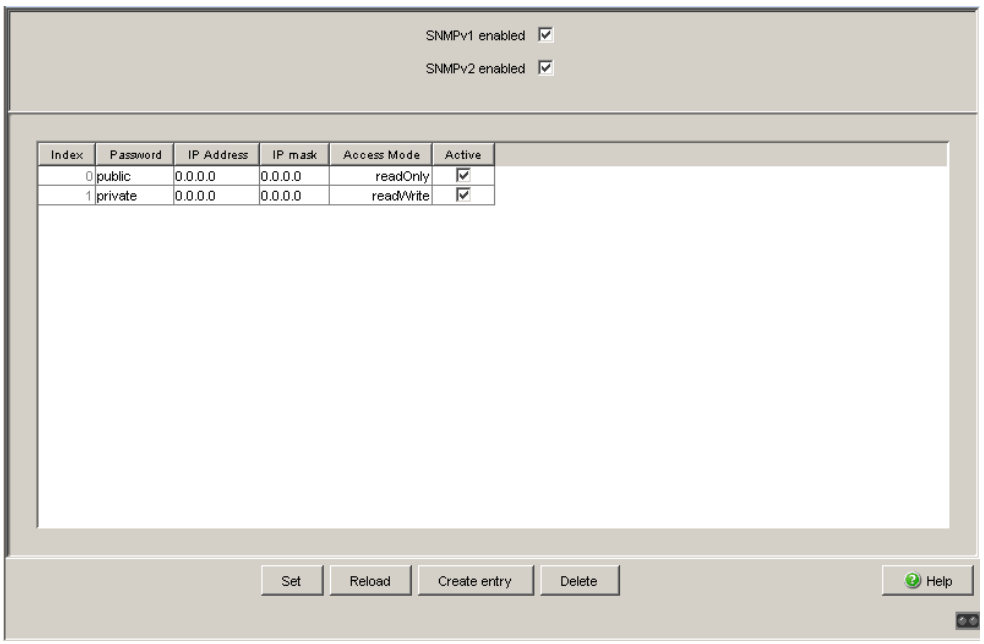


Figure 15: SNMPv1/v2 Access Dialog

2.3 Telnet/Web/SSH Access

This dialog allows you to switch off the Telnet server, the Web server and the SSH server on the device.

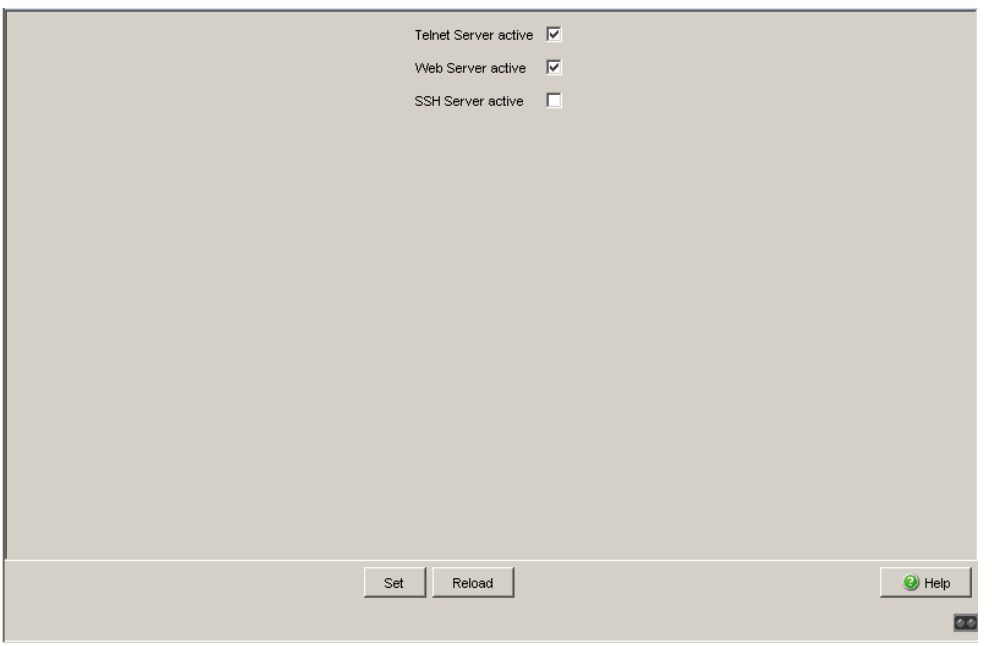


Figure 16: Telnet/Web/SSH Access dialog

2.3.1 Description of Telnet Access

The Telnet server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the Telnet server if you do not want Telnet access to the device.
On delivery, the server is activated.
After the Telnet server has been deactivated, you will no longer be able to access the device via a new Telnet connection. If a Telnet connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allow you to reactivate the Telnet server.

2.3.2 Description of Web Access

The Web server of the device allows you to configure the device by using the Web-based interface. Deactivate the Web server if you do not want the device to be accessed from the Web.
On delivery, the server is activated.

After the Web server has been switched off, it is no longer possible to log in via a Web browser. The login in the open browser window remains active.

Note: The Command Line Interface allows you to reactivate the Web server.

2.3.3 Description of SSH Access

The SSH server of the device allows you to configure the device by using the Command Line Interface (in-band). You can deactivate the SSH server to disable SSH access to the device.
On delivery, the server is deactivated.
After the SSH server has been deactivated, you will no longer be able to access the device via a new SSH connection. If an SSH connection already exists, it is kept.

Note: The Command Line Interface (out-of-band) and the `Security:Telnet/Web access` dialog in the Web-based interface allow you to reactivate the SSH server.

Note: To be able to access the device via SSH, you need a key that has to be installed on the device (see the "Basic Configuration" user manual).

2.4 Restricted Management Access

This dialog allows you to differentiate (restrict) the management access to the device based on IP address ranges and individual management services.

When you activate this function, you can only use the specified IP address ranges to access the management services activated for these address ranges. The device rejects other requests. You can create up to 16 entries in the list, permit or forbid specific management access for each address range, and activate or deactivate the individual entries separately.

The following management services support restricted management access:
- http
- snmp
- telnet
- ssh

Note: The CLI access via the V.24 interface is excluded from the function and cannot be restricted.

Note: You require the http service to start the Web-based interface in a browser.
Afterwards, you require the snmp service to access the device with the Web-based interface. When you start the Web-based interface outside the browser, you only require snmp.

In the default setting, the restricted management access is deactivated. In this case, anyone with the correct administrator logon data has access to all management services.

If you have activated the function, and if there is at least one active entry whose IP address range matches the request and for which the requested management service is allowed, the device processes the request. Otherwise the device rejects it.

In the state on delivery, the device provides you with a default entry with the IP address 0.0.0.0, the netmask 0.0.0.0 and all the management services. This allows access to all services from any IP address. This allows you full access to the device, even if a restriction is activated, e.g. to initially configure the function. You have the option to change or delete this entry.
When you create a new entry, this entry also has these preset properties.

Note: If you activate the function and no entry in the table permits your current access, then you can no longer access the management of the device once you write these settings to the device.
If no entry allows access, nobody has access to the device management. In this case, use the CLI access via V.24 to access the management of the device.

Variable	Meaning	Possible values	Default setting
Function	Switches the function on and off for the device.	`On`, `Off`	`Off`
Index	Sequential number of the entry. When you delete an entry, this leaves a gap in the numbering. When you create a new entry with the Web-based interface, the device fills the first gap.	1 - 16	1 (the preset entry).
IP Address	Together with the netmask, defines the network area for which this entry applies.	Valid IPv4 address or 0.0.0.0	0.0.0.0 (for all newly created entries)
Netmask	Together with the IP address, defines the network area for which this entry applies.	Valid IPv4 netmask or 0.0.0.0	0.0.0.0 (for all newly created entries)
HTTP	Activates or deactivates the http service (Web server) for this entry.	`On`, `Off`	`On` (for all newly created entries)
SNMP	Activates or deactivates the SNMP service (SNMP access) for this entry.	`On`, `Off`	`On` (for all newly created entries)
Telnet	Activates or deactivates the Telnet service (Telnet access) for this entry.	`On`, `Off`	`On` (for all newly created entries)
SSH	Activates or deactivates the SSH service (SSH access) for this entry.	`On`, `Off`	`On` (for all newly created entries)
Active	Activates or deactivates the entire entry.	`On`, `Off`	`On` (for all newly created entries)

Table 4: Restricted Management Access

Note: An entry with an IP address of 0.0.0.0 together with a netmask of 0.0.0.0 applies for all IP addresses.

2.5 Port Security

The device allows you to configure each port so that unauthorized access is prevented. Depending on your selection, the device checks the MAC address or the IP address of the connected device.

In the “Configuration” frame, you set whether the port security works with MAC or with IP addresses.

Name	Meaning
MAC-Based Port Security	Check source MAC address of the received data packet.
IP-Based Port Security	Translate source IP address when entering in MAC address and then check source MAC address of the received data packet.

Table 5: Configuration of port security globally for all ports

Set individual parameters for each port in the port table.

Name	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port Status	`enabled`: Port is switched on and transmitting. `disabled`: Port is switched off and not transmitting. The port is switched on if - an authorized address accesses the port or - an unauthorized address attempts to access the port and `trapOnly` or `none` is selected under “Action”. The port is switched off if - an unauthorized address attempts to access the port and `portDisable` is selected under “Action”.

Table 6: Configuration of port security for a single port

Name	Meaning
Allowed MAC Addresses	MAC addresses of the devices with which you allow data exchange at this port. The Web-based interface allows you to enter up to 10 MAC addresses, each separated by a space. After each MAC address you can enter a slash followed by a number identifying an address area. This number, between 2 and 47, indicates the number of relevant bits. Example: 00:80:63:01:02:00/40 stands for 00:80:63:01:02:00 to 00:80:63:01:02:FF or 00:80:63:00:00:00/24 stands for 00:80:63:00:00:00 to 00:80:63:FF:FF:FF If there is no entry, any number of devices can communicate via this port.
Current MAC Address	Shows the MAC address of the device from which the port last received data. The Web-based interface allows you to copy an entry from the “Current MAC Address” column into the “Allowed MAC Addresses” column by dragging and dropping with the mouse button.
Allowed IP Addresses	IP addresses of the devices with which you allow data exchange at this port. The Web-based interface allows you to enter up to 10 IP addresses, each separated by a space. If there is no entry, any number of devices can communicate via this port.
Action	Action performed by the device after an unauthorized access: – `none`: no action – `trapOnly`: send alarm – `portDisable`: disable the port with the corresponding entry in the port configuration table (see on page 27 “Port Configuration“) and send an alarm.

Table 6: Configuration of port security for a single port

Note: This entry in the port configuration table is part of the configuration (see on page 32 “Loading/Saving the Configuration“) and is saved together with the configuration.

Note: Prerequisites for the device to be able to send an alarm (trap) (see on page 231 “Alarms (Traps)“):
– You have entered at least one recipient
– You have selected at least one recipient in the “Active” column
– In the “Selection” frame, you have selected “Port Security”

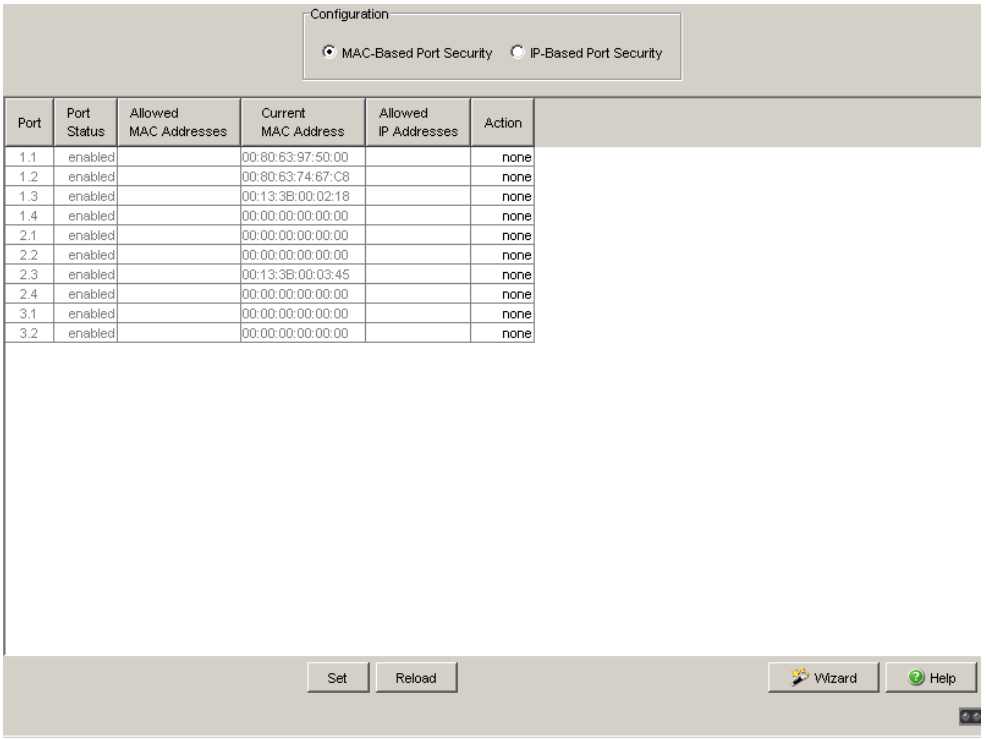


Figure 17: Port Security dialog

Note: The IP port security operates internally on layer 2. The device internally translates an allowed IP address into an allowed MAC address when you enter the IP address. An ARP request is used for this.

Prerequisites for the IP-based port security:
– The device with the allowed IP address supports ARP
– The device can be accessed while configuring IP port security
– The MAC address to which the IP address is assigned is unique and remains unchanged after the IP address is entered.

If you have entered a router interface as the allowed IP address, all the packets sent from this interface are considered allowed, since they contain the same MAC source address.

If a connected device sends packets with the allowed IP address but a different MAC address, it will not be allowed by the Switch. If you exchange the device with the allowed IP address for a different one with the same IP address, enter the IP address in the Switch again so that the Switch learns the new MAC address.

2.6 IEEE 802.1X Port Authentication

802.1x port authentication provides you with the following dialogs:
- “IEEE 802.1X Global“
- “IEEE 802.1X Port Configuration“
- “IEEE 802.1X Port Statistics“
- “RADIUS Server Settings for IEEE 802.1X“

The port-based network access control is a method described in the standard IEEE 802.1X to protect IEEE 802 networks from unauthorized access. The protocol controls the access to a port by authenticating and authorizing a device that is connected to this port of the device.
The authentication and authorization is performed by the authenticator, in this case the device. The device authenticates (or does not authenticate) the supplicant (the querying device, e.g. a PC), which means that it permits the access to the services it provides (e.g. access to the network to which the device is connected), or else refuses it. In the process, the device accesses an external authentication server (RADIUS server), which checks the authentication data of the supplicant. The device exchanges the authentication data with the supplicant via the Extensible Authentication Protocol over LANs (EAPOL), and with the RADIUS server via the RADIUS protocol.

2.6.1 IEEE 802.1X Global

The IEEE 802.1X Global dialog gives you the option of switching port authentication on or off.

☐ With "Function" you enable or disable the function.

☐ With "RADIUS Request Retransmissions” you specify, how often the device retransmits an unanswered request to the RADIUS server before the device transmits the request to another RADIUS server.

☐ With “RADIUS time-out” you specify how long (in seconds) the device waits for a response after a request to the RADIUS server before the device retransmits the request.

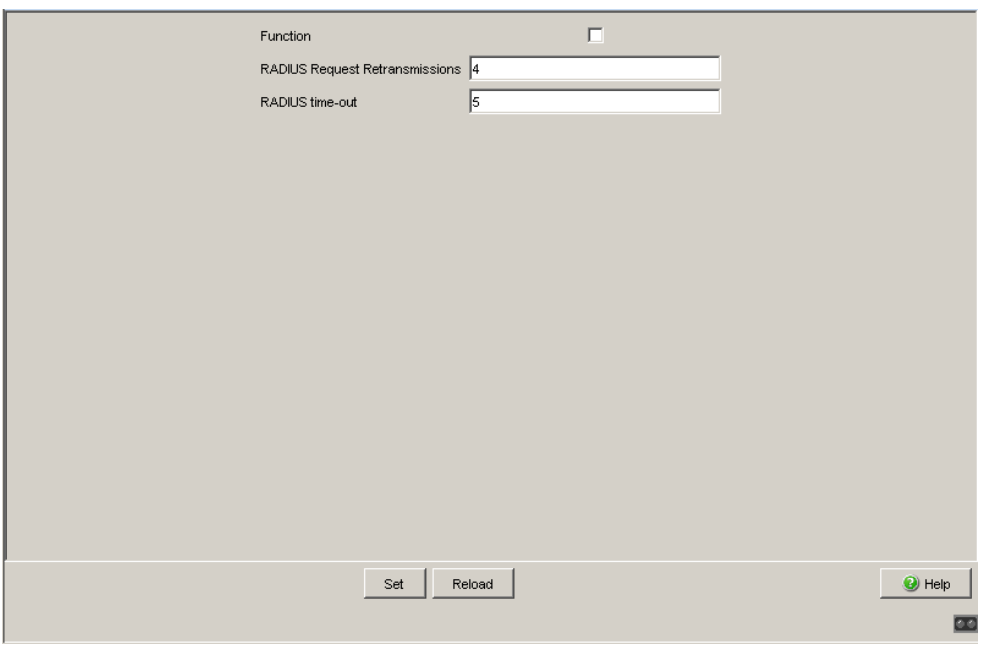


Figure 18: Global dialog

Preparing the device for the 802.1X port authentication

☐ Configure your own IP parameters (for the device).
☐ Globally enable the 802.1X port authentication function.
☐ Set the 802.1X port control to "auto". The default setting is "force-authorized".
☐ Enter the "shared secret" between the authenticator and the RADIUS server. The shared secret is a text string specified by the RADIUS server administrator.
☐ Enter the IP address and the port of the RADIUS server. The default UDP port of the RADIUS server is port 1812.

2.6.2 IEEE 802.1X Port Configuration

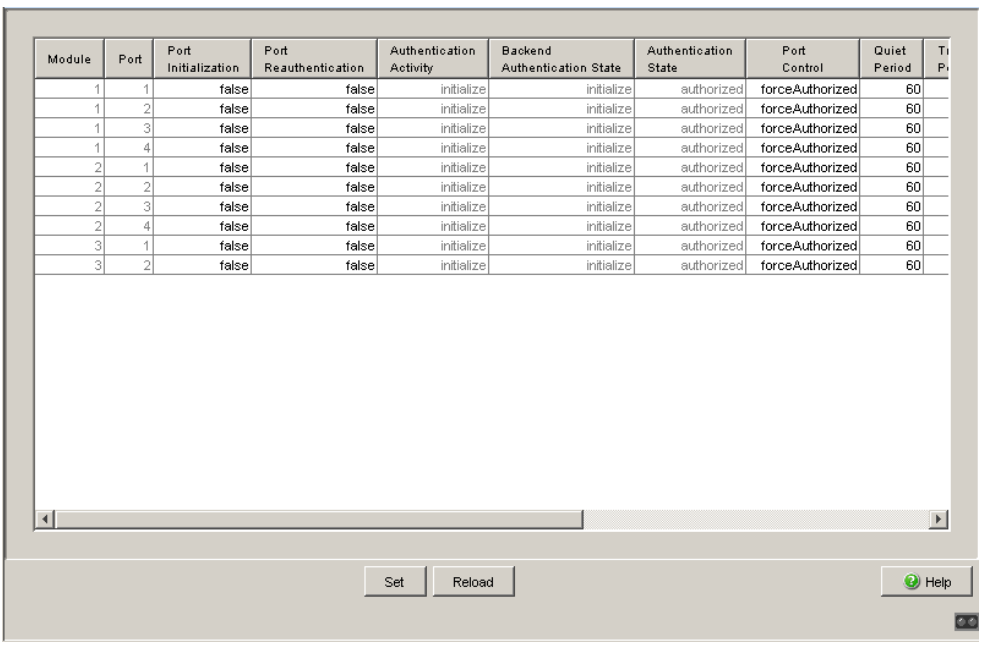

Module
Port
Port Initialization
Port Reauthentication
Authentication Activity
Backend Authentication State
Authentication State
Port Control
Quiet Period
1 1 false false initialize initialize authorized forceAuthorized 60
1 2 false false initialize initialize authorized forceAuthorized 60
1 3 false false initialize initialize authorized forceAuthorized 60
1 4 false false initialize initialize authorized forceAuthorized 60
2 1 false false initialize initialize authorized forceAuthorized 60
2 2 false false initialize initialize authorized forceAuthorized 60
2 3 false false initialize initialize authorized forceAuthorized 60
2 4 false false initialize initialize authorized forceAuthorized 60
3 1 false false initialize initialize authorized forceAuthorized 60
3 2 false false initialize initialize authorized forceAuthorized 60
Set
Reload
Help

Figure 19: Configuration table

Entries in the configuration table

Variable	Meaning	Possible values	State on delivery
Port Initialization	For resetting the initialization function. Setting this attribute to "true" causes the device to reset this function. When the resetting process is concluded, the value is reset to "false".	true, false	false
Port Reauthentication	To enable and disable the reauthentication for this port. Setting this attribute "true" causes the device to ask the supplicant reauthenticate itself on that port. Note: This attribute is reset to "false" after it has been read.	true, false	false
Authentication Activity	Displays the current value of the authentication activity.	1 = initialize 2 = disconnected 3 = connecting 4 = authenticating 5 = authenticated 6 = aborting authenticating 7 = held 8 = force authorized 9 = force unauthorized	
Server Authentication Status	Displays the current status of the authentication server.	1 = request 2 = response 3 = success 4 = failure (not authenticated) 5 = timeout 6 = idle 7 = initialize	
Authentication Status	Displays the current value of the authentication status for the port.	authorized = the connected subscriber has been authenticated unauthorized = the connected subscriber has not been authenticated	

Table 7: Setting options per port

Variable	Meaning	Possible values	State on delivery
Port Control	Setting for the port access control.	ForceAuthorized = access is granted without authentication. ForceUnauthorized = access is blocked even with authentication Auto = access according to the authentication result	ForceAuthorized
Idle Period	Period in seconds in which the authentication process does not expect authentication from the supplicants.	0-65535	60
Transmit Period	Wait period before the device sends an EAP packet again.	1-65535	30
Supplicant Timeout Period	Excess time in seconds for the communication between the device and the supplicant.	1-65535	30
Server Timeout	Excess time in seconds for the communication between the device and the server.	1-65535	30
Maximum Request Quantity	Maximum number of request attempts to the supplicants before the authentication process terminates.	1-10	2
Reauthentication Period	Period in seconds after which the device requests another authentication from the supplicant.	1-65535	3600
Reauthentication Enabled	Enabling or disabling reauthentication.	Marked Not marked	Not marked

Table 7: Setting options per port

2.6.3 IEEE 802.1X Port Statistics

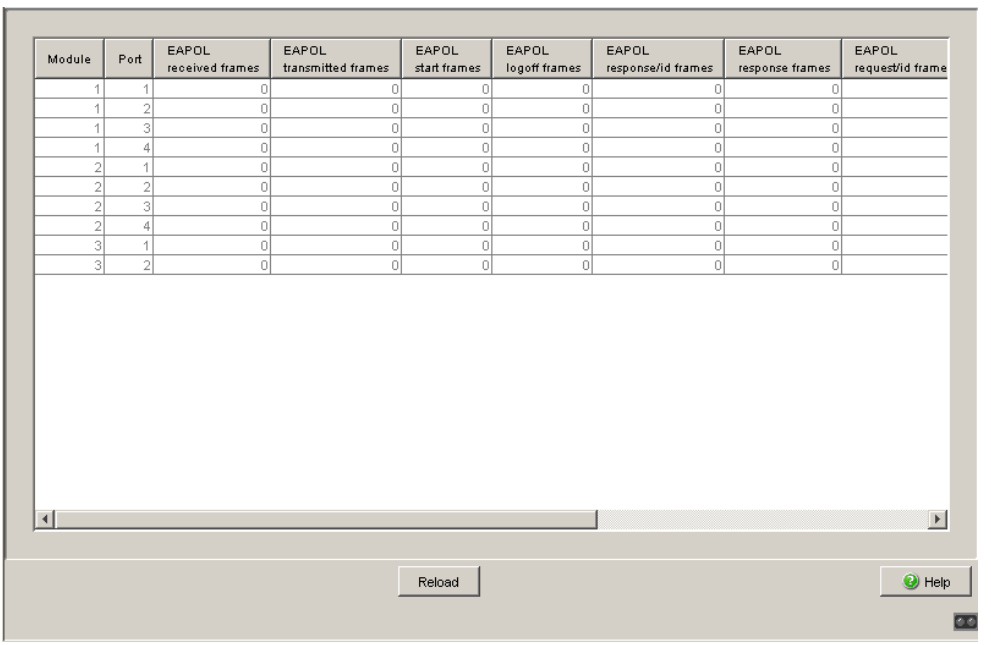

Module
Port
EAPOL received frames
EAPOL transmitted frames
EAPOL start frames
EAPOL logoff frames
EAPOL response/id frames
EAPOL response frames
EAPOL request/id frame
1 1 0 0 0 0 0 0
1 2 0 0 0 0 0 0
1 3 0 0 0 0 0 0
1 4 0 0 0 0 0 0
2 1 0 0 0 0 0 0
2 2 0 0 0 0 0 0
2 3 0 0 0 0 0 0
2 4 0 0 0 0 0 0
3 1 0 0 0 0 0 0
3 2 0 0 0 0 0 0
Reload
Help

Figure 20: Statistics table

Variable	Meaning
EAPOL received frames	Number of EAPOL frames (both valid and invalid) of any type that have been received at this port.
EAPOL transmitted frames	Number of EAPOL frames of any type that have been received at this port.
EAPOL start frames	Number of EAPOL start frames that have been received at this port.
EAPOL logoff frames	Number of EAPOL logoff frames that have been received at this port.
EAPOL response/ID Frames	Number of EAPOL resp/ID frames that have been received at this port.
EAPOL response frames	Number of valid EAP response frames (other than resp/ID frames) that have been received at this port.
EAPOL request/ID frames	Number of EAPOL req/ID frames that have been transmitted at this port.
EAPOL request frames	Number of EAP req/ID frames (other than req/ID frames) that have been transmitted at this port.
EAPOL invalid frames	Number of EAPOL frames with a frame type that is not recognized that have been transmitted at this port.
Received EAPOL error frames with invalid length specification	Number of EAPOL frames with an invalid packet body length field that have been transmitted at this port.
EAPOL frame version	The protocol version number carried in the last EAPOL frame received at this port.
Source address of the last received EAPOL frame	The MAC source address of the last received EAPOL frames 00:00:00:00:00:00 means: no frames received yet.

Table 8: Statistics table

2.6.4 RADIUS Server Settings for IEEE 802.1X

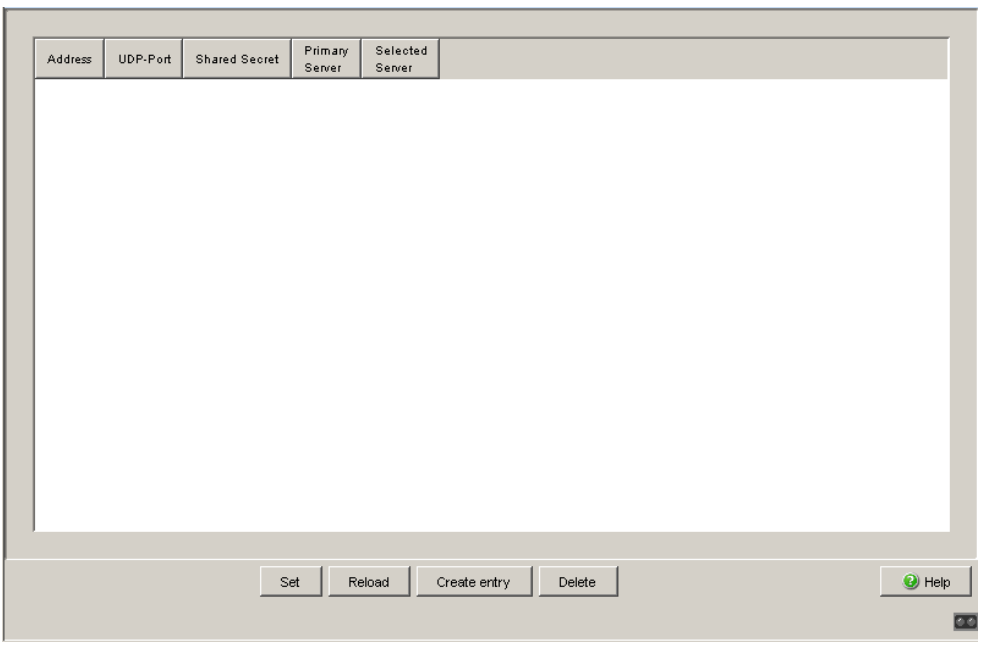


Figure 21: RADIUS Server dialog

This dialog allows you to enter the data for up to three RADIUS servers.

☐ Click on “Create entry” to open the dialog window for entering the IP address of a RADIUS server.

☐ Confirm the entered IP address with “OK”. This creates a new line in the table for this RADIUS server.

☐ In the “UDP port” column you enter the UDP port for the RADIUS server (the default setting is 1812).

☐ In the “Shared secret” column you enter the character string which you get as a key from the administrator of your RADIUS server.

☐ With “Primary server” you name this server as the first server which the Switch should contact for port authentication queries. If this server is not available, the device contacts the next server in the table.

- “Selected server” shows the server to which the Switch actually sends its queries.
- With “Delete entry” you delete the selected line in the table.

3 Time

With this dialog you can enter time-related settings independently of the time synchronization protocol selected.

- The “IEEE/SNTP time” displays the time with reference to Universal Time Coordinated (UTC).
  The time displayed is the same worldwide. Local time differences are not taken into account.

- The “System time” uses the “IEEE 1588 / SNTP time”, allowing for the local time difference from “IEEE 1588 / SNTP time”.
  “System time” = “IEEE 1588 / SNTP time” + “Local offset”.

- “Time source” displays the source of the following time data. The device automatically selects the source with the greatest accuracy.
  Possible sources are: `local` and `sntp`. The source is initially `local`. If SNTP is activated and if the device receives a valid SNTP packet, the device sets its time source to `sntp`.

☐ With “Set time from PC”, the device takes the PC time as the system time and calculates the IEEE 1588 / SNTP time using the local time difference.
“IEEE 1588 / SNTP time” = “System time” - “Local offset”

- The “Local Offset” is for displaying/entering the time difference between the local time and the “IEEE 1588 / SNTP time”.

☐ With “Set offset from PC”, the agent determines the time zone on your PC and uses it to calculate the local time difference.

Note: When setting the time in zones with summer and winter times, make an adjustment for the local offset, if applicable. The device can also get the SNTP server IP address and the local offset from a DHCP server.

Interaction of PTP and SNTP

According to PTP (IEEE 1588) and SNTP, both protocols can exist in parallel in the same network. However, since both protocols affect the system time of the device, situations may occur in which the two protocols compete with each other.

The PTP reference clock gets its time either via SNTP or from its own clock. All other clocks favor the PTP time as the source.

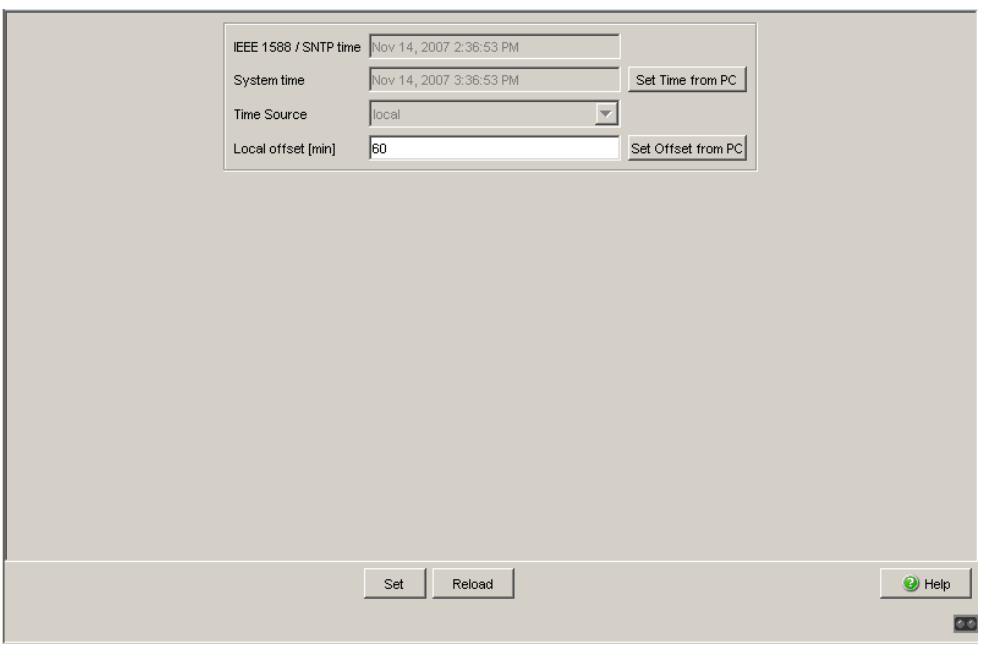


Figure 22: Time Dialog

3.1 SNTP configuration

The Simple Network Time Protocol (SNTP) enables you to synchronize the system time in your network.
The device supports the SNTP client and the SNTP server function.
The SNTP server makes the UTC (Universal Time Coordinated) available. UTC is the time relating to the coordinated world time measurement. The time displayed is the same worldwide. Local time differences are not taken into account.
The SNTP client obtains the UTC from the SNTP server.

Note: For the most accurate system time distribution possible, only use network components (routers, switches, hubs) which support SNTP in the signal path between the SNTP server and the SNTP client.

Parameter	Meaning	Possible Values	Default Setting
Function	Switches the SNTP function on and off globally.	`On, Off`	`Off`

Table 9: Switches SNTP on and off globally

Parameter	Meaning	Possible Values	Default Setting
SNTP Status	Displays conditions such as “Server cannot be reached”.	-	-

Table 10: SNTP Status

Parameter	Meaning	Possible Values	Default Setting
Client Status	Switches the SNTP client on and off.	`On, Off`	`On`
External server address	IP address of the SNTP server from which the device periodically requests the system time.	Valid IPv4 address	0.0.0.0
Redundant server address	IP address of the SNTP server from which the device periodically requests the system time if it does not receive a response to a request from the “External server address” within 0.5 seconds.	Valid IPv4 address	0.0.0.0
Server request interval	Time interval at which the device requests SNTP packets	1 s - 3,600 s	30 s
Accept SNTP Broadcasts	Specifies whether the device accepts the system time from SNTP Broadcast/Multicast packets that it receives.	`On, Off`	`On`
Threshold for obtaining the UTC [ms]	The device changes the time as soon as the deviation from the server time is above this threshold in milliseconds. This reduces the frequency of time changes.	0 - 2.147.483.647 (2^{31}-1)	0
Disable client after successful synchronization	Enable/disable further time synchronizations once the client, after its activation, has synchronized its time with the server. **Note:** If you have enabled PTP at the same time, the SNTP client first collects 60 time stamps before it deactivates itself. The device thus determines the drift compensation for its PTP clock. With the preset server request interval, this takes about half an hour.	`On, Off`	`Off`

Table 11: Configuration SNTP Client

Note: If you are receiving the system time from an external/redundant server address, switch off the reception of SNTP Broadcasts (see “Accept SNTP Broadcasts”). You thus ensure that the device only takes the time from a defined SNTP server.

Parameter	Meaning	Possible Values	Default Setting
Server status	Switches the SNTP server on and off.	`On, Off`	`On`
Anycast destination address	IP address, to which the SNTP server of the device sends the SNTP packets (see table 13).	Valid IPv4 address	0.0.0.0
VLAN ID	VLANs to which the device periodically sends SNTP packets.		1
Anycast send interval	Time interval at which the device sends SNTP packets.	1 - 3,600	120
Disable Server at local time source	Enables/disables the SNTP server function if the status of the time source is `local` (see Time dialog).	`On, Off`	`Off`

Table 12: Configuration SNTP Server

IP destination address	Send SNTP packet to
0.0.0.0	Nobody
Unicast address (0.0.0.1 - 223.255.255.254)	Unicast address
Multicast address (224.0.0.0 - 239.255.255.254), especially 224.0.1.1 (NTP address)	Multicast address
255.255.255.255	Broadcast address

Table 13: Destination address classes for SNTP packets

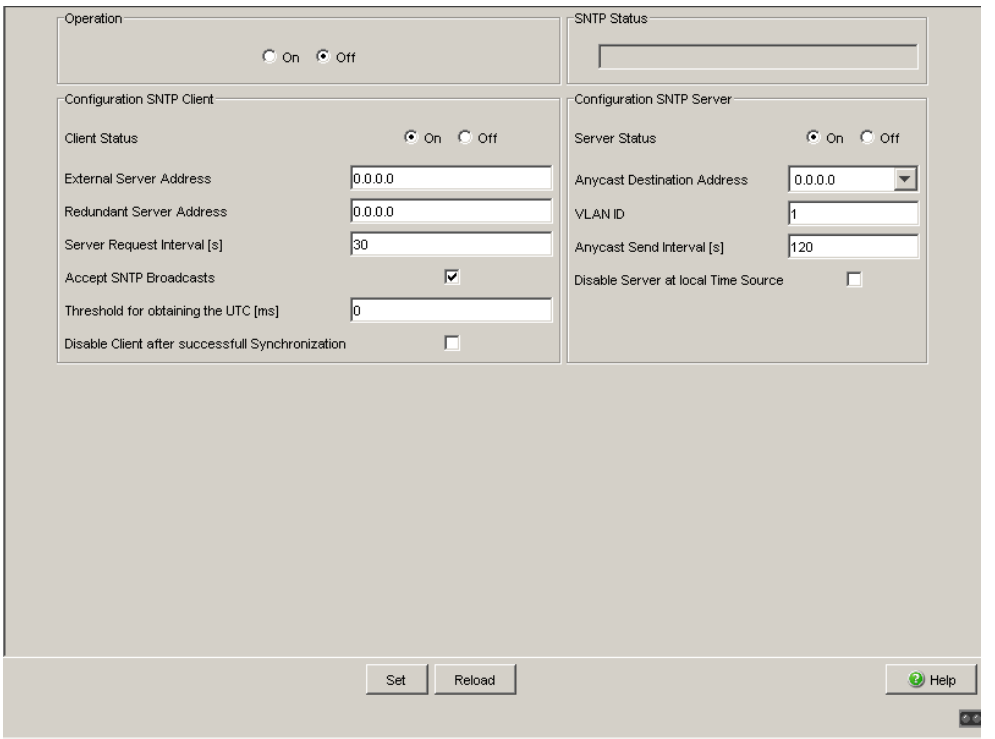


Figure 23: SNTP Dialog

3.2 PTP (IEEE 1588)

Precise time management is required for running time-critical applications via a LAN.
The IEEE 1588 standard with the Precision Time Protocol (PTP) describes a procedure that assumes one clock is the most accurate and thus enables precise synchronization of all clocks in a LAN.

For devices **without** a real-time (RT) module (module without timestamp unit):

- enable/disable the PTP function in the `PTP` dialog.
- select PTP mode in the `PTP` dialog.
  - Select `v1-simple-mode` if the reference clock uses PTP Version 1.
  - Select `v2-simple-mode` if the reference clock uses PTP Version 2.

The following sections apply to devices **with** support of real-time (RT) modules (modules with timestamp unit).

3.2.1 PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

The table below helps you to select the PTP version and the PTP mode.

Version	Mode	Reference clock used	Device with timestamp	PTP messages
Version 1	v1-simple-mode	Version 1	No	—
	v1-boundary-clock	Version 1	Yes	Process
Version 2	v2-simple-mode	Version 2	No	—
	v2-boundary-clock-onestep	Version 2	Yes	Process
	v2-boundary-clock-twostep	Version 2	Yes	Process
	v2-transparent-clock	Version 2	Yes	Forward

Table 14: Selecting the PTP version and the PTP mode

The PTP modes
- `v1-boundary-clock`,
- `v2-boundary-clock-onestep`,
- `v2-boundary-clock-twostep` and
- `v2-transparent-clock`

enable you to optimize the accuracy of the time.

You use these dialogs here
- Version 1
- Version 2 (Boundary Clock, BC)
- Version 2 Transparent Clock, (TC)

The PTP modes
- `v1-simple-mode` and
- `v2-simple-mode`

allow you to use the plug-and-play start-up.

Parameter	Meaning	Possible Values	Default Setting
Function on/off	Enable/disable the PTP function	On, Off	Off

Table 15: Function IEEE 1588/PTP

Parameter	Meaning	Possible Values	Default Setting
PTP version/ mode	Version and mode of the local clock.		v1-boundary-clock
	Boundary Clock function based on IEEE1588-2002 (PTPv1).	v1-boundary-clock	
	Support for PTPv1 without special hardware. The device synchronizes itself with received PTPv1 messages. This mode does not provide any other functions, such as PTP management or runtime measuring. Select this mode if the device does not have a timestamp unit (RT module).	v1-simple-mode	
	Boundary Clock function based on IEEE1588-2008 (PTPv2). The one-step mode determines the precise PTP time with 1 message. This mode is available for MM23 and MM33 modules.	v2-boundary-clock-onestep	
	Boundary Clock function based on IEEE1588-2008 (PTPv2). The two-step mode determines the precise PTP time with 2 messages.	v2-boundary-clock-twostep	
	Transparent Clock (one-step) function based on IEEE1588-2008 (PTPv2). This mode is available for MM23 and MM33 modules.	v2-transparent-clock	
	Support for PTPv2 without special hardware. The device synchronizes itself with received PTPv2 messages. This mode does not provide any other functions, such as PTP management or runtime measuring. Select this mode if the device does not have a timestamp unit (RT module).	v2-simple-mode	

Table 16: Configuration IEEE 1588/PTP

Parameter	Meaning	Possible Values	Default Setting
Bottom synchronization threshold [ns]	Bottom PTP synchronization threshold value, specified in nanoseconds. If the result of (reference time - local time) is lower than the value of the bottom PTP synchronization threshold, then the local clock is deemed as synchronous with the reference clock.	0-999.999.999	30
Top synchronization threshold [ns]	Top PTP synchronization threshold value, specified in nanoseconds. If the result of (reference time - local time) is greater than the value of the top PTP synchronization threshold, then the local clock is deemed as not being synchronous with the reference clock.	31-1.000.000.000	5000

Table 16: Configuration IEEE 1588/PTP

Parameter	Meaning	Possible Values	Default Setting
Is synchronized	Local clock synchronized with reference clock; compare `Bottom synchronization threshold` and `Top synchronization threshold`.	true false	
Max Offset absolute [ns]	Total deviation of the local clock from the reference clock in nanoseconds since the local clock was last reset. The local clock is reset with “Reinitialize” in this dialog or by resetting the device.		

Table 17: IEEE 1588/PTPStatus

3.2.2 PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

You select the PTP version you will use in the `Time:PTP:Global` dialog.

PTP Version 1, Global Settings

Parameter	Meaning	Possible Values	Default Setting
Sync Interval	Period for sending synchronization messages. Entered in seconds.	- sec-1 - sec-2 - sec-8 - sec-16 - sec-64	sec-2
Subdomain name	Name of the PTP subdomain to which the local clock belongs.	1 to 16 ASCII characters, hex value 0x21 (!) through 0x7e (~)	_DFLT
Preferred Master	Defines the local clock as the preferred master. If PTP does not find another preferred master, then the local clock is used as the grandmaster clock. If PTP finds other preferred masters, then PTP determines which of the preferred masters is used as the grandmaster clock.	true false	false

Table 18: Function IEEE 1588/PTPv1

Parameter	Meaning	Possible Values	Default Setting
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Runtime to Master [ns]	Single signal runtime between the local device and reference clock in nanoseconds.		
Grandmaster UUID	MAC address of the grandmaster clock (Unique Universal Identifier).		
Parent UUID	MAC address of the master clock with which the local time is directly synchronized.		
Clock Stratum	Qualification of the local clock.		
Clock identifier	Clock properties (e.g accuracy, epoch, etc.).		

Table 19: Status IEEE 1588/PTPv1

PTP Version 1, Port Settings

Parameter	Meaning	Possible Values	Default Setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. The table remains empty if the device does not support the PTP mode selected		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	
PTP Burst on	2 to 8 synchronization runs take place during the synchronization interval. This enables faster synchronization with a correspondingly higher network load.	on	off
	One synchronization run is performed in a synchronization interval.	off	
PTP Status	Port is in the initialization phase.	initializing	
	A PTP protocol error was detected on this port.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP passive mode.	passive	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP slave mode.	slave	

Table 20: Port dialog version 1

3.2.3 PTP Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

PTP version 2 provides considerably more settings. These support
- faster reconfiguration of the PTP network than in PTP version 1
- greater precision in some environments.

You select the PTP version you will use in the `Time:PTP:Global` dialog.

Global

Parameter	Meaning	Possible Values	Default Setting
Priority 1	The clock with the lowest priority 1 becomes the reference clock (grandmaster).	0-255	128
Priority 2	If all the relevant values for selecting the reference clock are the same for multiple devices, the clock with the lowest priority 2 is selected as the reference clock (grandmaster).	0-255	128
Domain number	Assignment of the clock to a PTPv2 domain. Only clocks with the same domain are synchronized.	0-255	0

Table 21: Function IEEE 1588/PTPv2 BC

Parameter	Meaning	Possible Values	Default Setting
Two Step	Displays the clock mode of the device		No
	v2-boundary-clock-onestep	No	
	v2-boundary-clock-twostep	Yes	
Number of BCs to grandmaster	Number of boundary clocks between PTP reference clock and this device		
Offset to Master [ns]	Deviation of the local clock from the reference clock in nanoseconds.		
Runtime to Master [ns]	Single signal runtime between the local device and the reference clock in nanoseconds. The display depends on the port setting “Runtime measuring mechanism”.		

Table 22: Status IEEE 1588/PTPv2 BC

Parameter	Meaning	Possible Values	Default Setting
Clock identifier	Own UUID (unique identification number)		
Parent port identifier	UUID of the direct master		
Grandmaster identifier	UUID of the reference clock		

Table 23: Identifiers

Parameter	Meaning	Possible Values	Default Setting
Priority 1	Display priority 1 of the current reference clock.		
Priority 2	Display priority 2 of the current reference clock.		
Class	Class of the reference clock		
Precision	Estimated accuracy with regard to UTC		
Variance	Variance as described in the IEEE1588-2008 standard		

Table 24: Grandmaster (reference clock)

Parameter	Meaning	Possible Values	Default Setting

Time source	Source selected for own clock.	`atomicClock`
		`gps`
		`terrestrialRadio`
		`ptp`
		`ntp`
		`handset`
		`other`
		`internalOscillator`
			`internalOscillator`

UTC Offset [s]	Current difference between the PTP time scale (see below) and the UTC.	-2,147,483,648 to 2,147,483,647	34
UTC Offset valid	Specifies whether value of UTC offset is valid or not.	`Yes, No`	`No`
Time Traceable	The device gets the time from a primary UTC reference, e.g. from an NTP server.	`Yes, No`	
Frequency Traceable	The device gets the frequency from a primary UTC reference, e.g. NTP server, GPS.	`Yes, No`	
PTP Time Scale	The device uses the PTP time scale. According to IEEE 1588, the PTP time scale is the TAI atomic time started on January 01, 1970. In contrast to UTC, TAI does not use leap seconds On January 01, 2010, the difference between TAI and UTC was +34 seconds.	`Yes, No`	

Table 25: Properties of the Local Time

Port

Parameter	Meaning	Possible Values	Default Setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. If the device does not support the PTP mode selected, the table is empty.		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages.	off	
PTP Status	Port is in the initialization phase.	initializing	
	A PTP protocol error was detected on this port.	faulty	
	PTP function is switched off at this port.	disabled	
	Port has not received any information and is waiting for synchronization messages.	listening	
	Port is in PTP pre-master mode.	pre-master	
	Port is in PTP master mode.	master	
	Port is in PTP uncalibrated mode.	uncalibrated	
	Port is in PTP passive mode.	passive	
	Port is in PTP slave mode.	slave	
E2E Runtime Measuring Interval	Displays in seconds the interval for E2E (End-to-End) runtime measurements at this port. This is a value for the device, assigned to ports with the PTP status Slave by the connected master. If the port itself is the master, then the device assigns the port the value 8 (state on delivery).		8
P2P Runtime	Measured P2P (Peer-to-Peer) runtime. Prerequisite: you have selected the P2P runtime measuring mechanism.		
Announce Interval	Interval of the messages for PTP topology discovery (selection of the reference clock). Select the same value for all devices within a PTP domain.	1, 2, 4, 8, 16	2

Table 26: Port Dialog Version 2(BC)

Parameter	Meaning	Possible Values	Default Setting
Announce Timeout	Announce interval timeout for PTP topology discovery in number of announce intervals. The standard settings of announce interval = 2 (2 per second) and announce timeout = 3 lead to a timeout of 3 x 2 seconds = 6 seconds. Select the same value for all devices within a PTP domain.	2-10	3
Sync Interval	Interval in seconds for the synchronization messages	`0.5; 1; 2`	`1`
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	The device itself does not generate any messages in the runtime measurement. A connected PTP slave measures the runtime of the entire transmission path to the master.	`E2E` (End-to-End):	
	The device itself measures the runtime to all the connected PTP devices. If a reconfiguration is performed, this eliminates the need to determine the runtime again. The MICE media modules MM23 and MM33 support the P2P mechanism.	`P2P` (Peer-to-Peer)	
	No runtime determination.	Disabled	
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the connected PTP device.		
Network Protocol	Transport protocol for PTP messages.	`802.3 Ethernet`, `UDP/IPv4`	`UDP/IPv4`

Table 26: Port Dialog Version 2(BC)

Parameter	Meaning	Possible Values	Default Setting
V1 Hardware Compatibility	Some devices from other manufacturers require PTP messages of specific length. If the UDP/IPv4 network protocol is selected and the function is active, the device extends the PTP messages.	auto, on, off	auto
Asymmetry	Correction of the runtime asymmetry in ns. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x·2 ns		

Table 26: Port Dialog Version 2(BC)

3.2.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE)

In strongly cascaded networks in particular, the transparent clock (TC) introduced in PTP Version 2 provides a noticeable increase in precision. The combination with the P2P runtime mechanism (simultaneous runtime measurement at all ports) enables “seamless” reconfiguration.

The following settings enable you to also use the TC for Unicast PTP messages:
– Selecting the E2E mechanism
– Syntonize disabled
– PTP Management disabled.

You select the PTP version you will use in the `Time:PTP:Global` dialog.

PTP Version 2 (TC), Global Settings

Parameter	Meaning	Possible Values	Default Setting
Runtime Measuring Mechanism	Mechanism for measuring the message runtime. Enter the same mechanism for the PTP device connected to this port.		
	The device itself does not generate any messages in the runtime measurement. A connected PTP slave measures the runtime of the entire transmission path to the master.	`E2E` (End-to-End):	
	The device itself measures the runtime to all the connected PTP devices. If a reconfiguration is performed, this eliminates the need to determine the runtime again.	`P2P` (peer-to-peer)	
	Primary Domain	Assignment of the clock to a PTPv2 domain.	0-225
Multi Domain Mode	TC corrects messages from all domains.	`Yes`	`Yes`
	TC only corrects messages from the primary domain.	No	
Network Protocol	Network protocol for P2P and management messages.	udplpv4 ieee8023	udplpv4
Syntonize	Synchronize frequency.	Yes No	No
PTP Management	Activate/deactivate the PTP management. To reduce the load on the device, deactivate PTP Management and Syntonize - at high synchronization rates and - in Unicast mode.	Yes No	Yes

Table 27: Function IEEE 1588 / PTPv2 TC

Parameter	Meaning	Possible Values	Default Setting
Clock identifier	UUID of the TC (transparent clock)		
Current master	If Syntonize is enabled, displays the UUID of the master with which the device synchronizes its frequency.		

Table 28: Status IEEE 1588 / PTPv2 TC

PTP Version 2 (TC), Port Settings

Parameter	Meaning	Possible Values	Default Setting
Module	Module number for modular devices, otherwise 1.		
Port	Port to which this entry applies. If the device does not support the PTP mode selected, the table is empty.		
PTP on	Port sends/receives PTP synchronization messages	on	on
	Port blocks PTP synchronization messages. The device does not process any PTP messages it receives at this port.	off	
P2P Runtime Measuring Interval	Interval for peer-to-peer runtime measurements at this port. Prerequisite: You have selected the P2P runtime measuring mechanism on the device itself and on the connected PTP device.		
P2P Runtime	Measured P2P (Peer-to-Peer) runtime. Prerequisite: you have selected the P2P runtime measuring mechanism.		
Asymmetry	Correction of the runtime asymmetry in ns. A runtime measurement value of x ns corrupted by asymmetrical transmission values corresponds to an asymmetry of x·2 ns		

Table 29: Port Dialog Version 2(TC)

4 Switching

The switching menu contains the dialogs, displays and tables for configuring the switching settings:

- Switching Global
- Filters for MAC Addresses
- Rate Limiter
- Multicasts
- VLAN

4.1 Switching Global

Variable	Meaning	Possible Values	
MAC address (read only)	Display the MAC address of the device		
Aging Time (s)	Enter the Aging Time in seconds for dynamic MAC address entries. In connection with the router redundancy, select a time ≥ 30 s.	PowerMICE, MACH 104, MACH 1040, MACH 4000: 10-630 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 15-3.825	30
Flow control	Activate/deactivate the flow control **Note:** When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on all ports. If the flow control and the redundancy function are active at the same time, there is a risk of the redundancy failing.	`On`, `Off`	`Off`
Learning addresses	Activate/deactivate the learning of MAC source addresses.	`On`, `Off`	`On`
Frame size	Set the maximum packet size (frame size) in bytes.	PowerMICE, MACH 104, MACH 1040, MACH 4000: 1522, 1552 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 1522, 1632	1522

Table 30: Switching:Global dialog

Variable	Meaning	Possible Values	
Activate Address Relearn Detection	Enable/disable whether the device detects whether it has repeatedly learned the same MAC source addresses at different ports. This process very probably indicates a loop situation in the network. If the device detects this process, it creates an entry in the log file and sends an alarm (trap).	`On`, `Off`	`Off`
Address Relearn Threshold	Number of MAC addresses that are learned at different ports within a checking interval, so that if this number is exceeded, the device sees this as a relevant event. The interval for this check is a few seconds.	1 - 1,024	1
Activate Duplex Mismatch Detection	Enable/disable whether the device reports a duplex problem at a port for specific error events. This means that the duplex mode of the port might not match that of the remote port. If the device detects a potential non-match, it creates an entry in the event log and sends an alarm (trap). To detect potential non-matches, the device evaluates the error counters of the port after the connection is set up, in the context of the port settings (see table 31).	`On`, `Off`	`Off`

Table 30: Switching:Global dialog

The following table lists the duplex operating modes for TX ports together with the possible error events. The terms in the table mean:

- Collisions: In half-duplex mode, collisions mean normal operation.
- Duplex problem: Duplex modes do not match.
- EMI: Electromagnetic interference.
- Network extension: The network extension too great, or too many hubs are cascaded.

- Collisions, late collisions: In full-duplex mode, the port does not count collisions or late collisions.
- CRC error: The device only evaluates these errors as duplex problems in the manual full duplex mode.

No.	Autonegotiation	Current duplex mode	Detected error events (≥ 10)	Evaluation of duplex situation by device	Possible causes
1	On	Half duplex	None	OK	
2	On	Half duplex	Collisions	OK	
3	On	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
4	On	Half duplex	CRC error	OK	EMI
5	On	Full duplex	None	OK	
6	On	Full duplex	Collisions	OK	EMI
7	On	Full duplex	Late collisions	OK	EMI
8	On	Full duplex	CRC error	OK	EMI
9	Off	Half duplex	None	OK	
10	Off	Half duplex	Collisions	OK	
11	Off	Half duplex	Late collisions	Duplex problem detected	Duplex problem, EMI, network extension
12	Off	Half duplex	CRC error	OK	EMI
13	Off	Full duplex	None	OK	
14	Off	Full duplex	Collisions	OK	EMI
15	Off	Full duplex	Late collisions	OK	EMI
16	Off	Full duplex	CRC error	Duplex problem detected	Duplex problem, EMI

Table 31: Evaluation of non-matching of the duplex mode

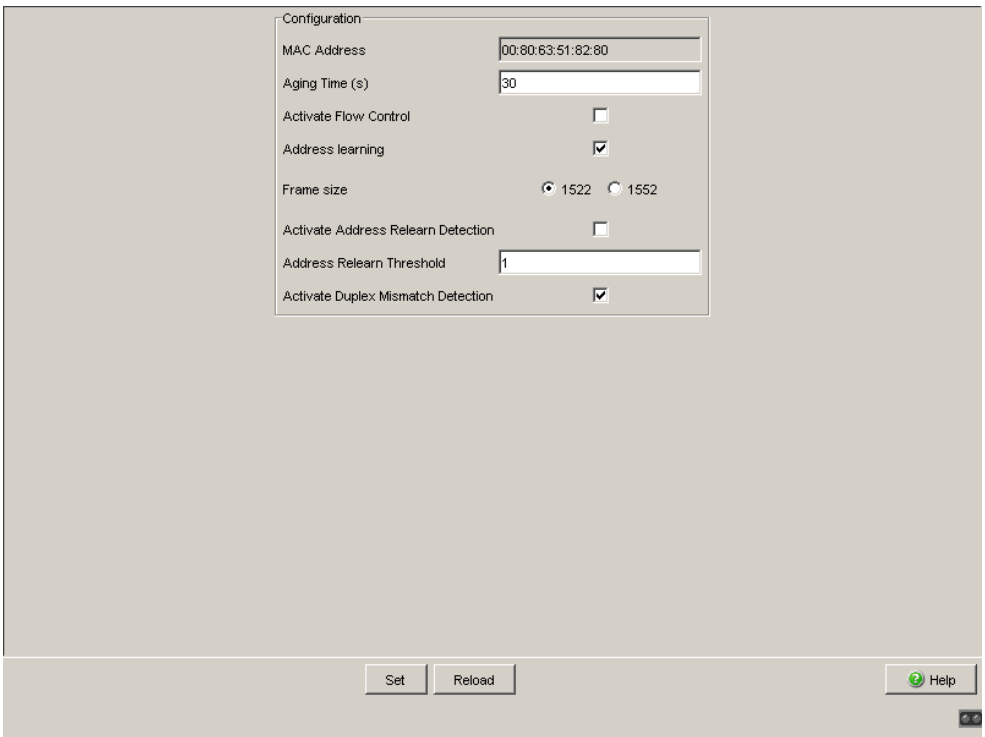


Figure 24: Dialog Switching Global

4.2 Filters for MAC addresses

The filter table for MAC addresses is used to display and edit filters. Each row represents one filter. Filters specify the way in which data packets are sent. They are set automatically by the device (learned status) or manually. Data packets whose destination address is entered in the table are sent from the receiving port to the ports marked in the table. Data packets whose destination address is not in the table are sent from the receiving port to all other ports. The following conditions are possible:

- `learned`: The filter was created automatically by the device.
- `invalid`: With this status you delete a manually created filter.
- `permanent`: The filter is stored permanently in the device or on the URL (see on page 32 “Loading/Saving the Configuration“).
- `gmrp`: The filter was created by GMRP.
- `gmrp/permanent`: GMRP added further port markings to the filter after it was created by the administrator. The port markings added by the GMRP are deleted by a restart.
- `igmp`: The filter was created by IGMP Snooping.

In the “Create” dialog (see buttons below), you can create new filters.

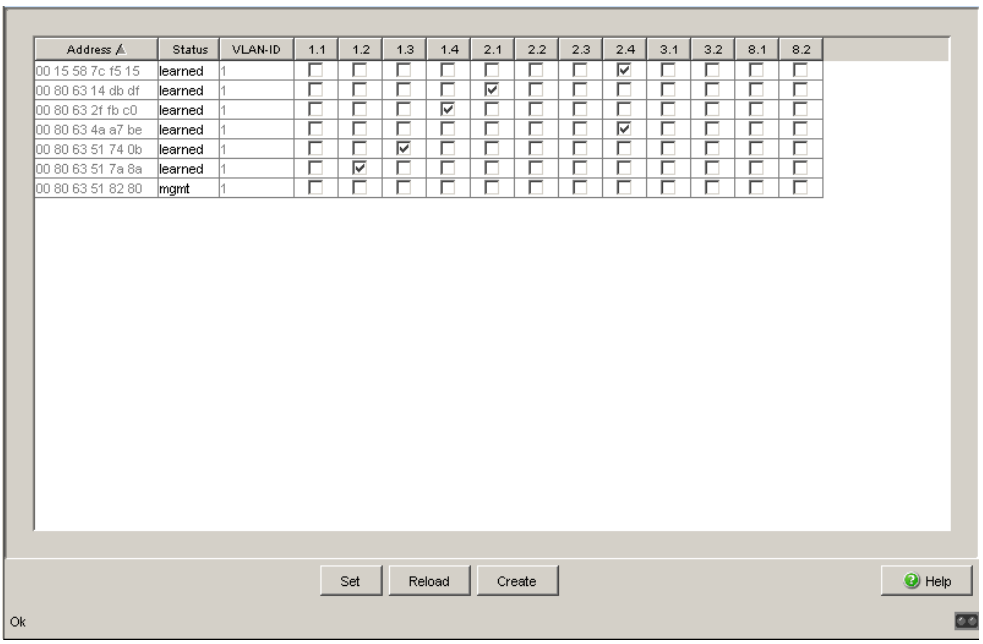


Figure 25: Filter Table dialog

Note: For Unicast addresses, the PowerMICE, MACH 1040 and MACH 4000 devices allow you to include multiple ports in a filter entry. Do not include any ports if you want to create a discard filter entry.

Note: This filter table allows you to create up to 100 filter entries for Multicast addresses.

4.3 Rate Limiter

The device can limit the rate of message traffic during periods of heavy traffic flow.

Entering a limit rate for each port specifies the amount of traffic the device is permitted to transmit and receive.

If the data load transmitted at this port exceeds the maximum load entered, the device will discard the excess data at this port.

A global setting enables/disables the rate limiter function at all ports.

Note: The limiter functions work exclusively on layer 2 and serve the purpose of limiting the effects of storms of those frame types (typically broadcasts) that the Switch floods. The limiter function ignores any protocol information of higher layers like IP or TCP. This may affect e.g., TCP traffic.

You can minimize this effects by:

- applying the limiter function only to particular frame types (e.g., to broadcasts, multicasts and unicasts with an unlearned destination address) and excluding unicasts with a learned destination address from the limitation,
- using the egress limiter function instead of the ingress limiter function because the former cooperates slightly better with TCP‘s flow control (reason: frames buffered by the internal switching buffer),
- increasing the aging time for learned unicast destination addresses.

Note: Ports that are included in a Link Aggregation (see page 136) are excluded from the rate limitation, regardless of the entries in the “Rate Limiter” dialog.

4.3.1 Rate Limiter settings for RS20/RS30/40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS

- "Ingress Limiter (kbit/s)" allows you to enable or disable the input limiting function for all ports.
- "Egress Limiter (Pkt/s)" allows you to enable or disable the broadcast output limiter function at all ports.
- "Egress Limiter (kbit/s)" allows you to enable or disable the output limiter function for all packet types at all ports.

Setting options per port:

- "Ingress Packet Types" allows you to select the packet type for which the limit is to apply:
  - `All`, limits the total inbound data volume at this port.
  - `BC`, limits the broadcast packets received at this port.
  - `BC + MC`, limits broadcast packets and Multicast packets received at this port.
  - `BC + MC + uUC`, limits broadcast packets, Multicast packets, and unknown Unicast packets received at this port.
- Ingress Limiter Rate for the inbound packet type selected:
  - = 0, no ingress limit at this port.
  - > 0, maximum inbound traffic rate in kbit/s that can be received at this port.
- Egress Limiter Rate for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outbound broadcasts per second that can be sent at this port.
- Egress Limiter Rate for the entire data stream:
  - = 0, no rate limit for outbound data stream at this port.
  - > 0, maximum outbound transmission rate in kbit/s sent at this port.

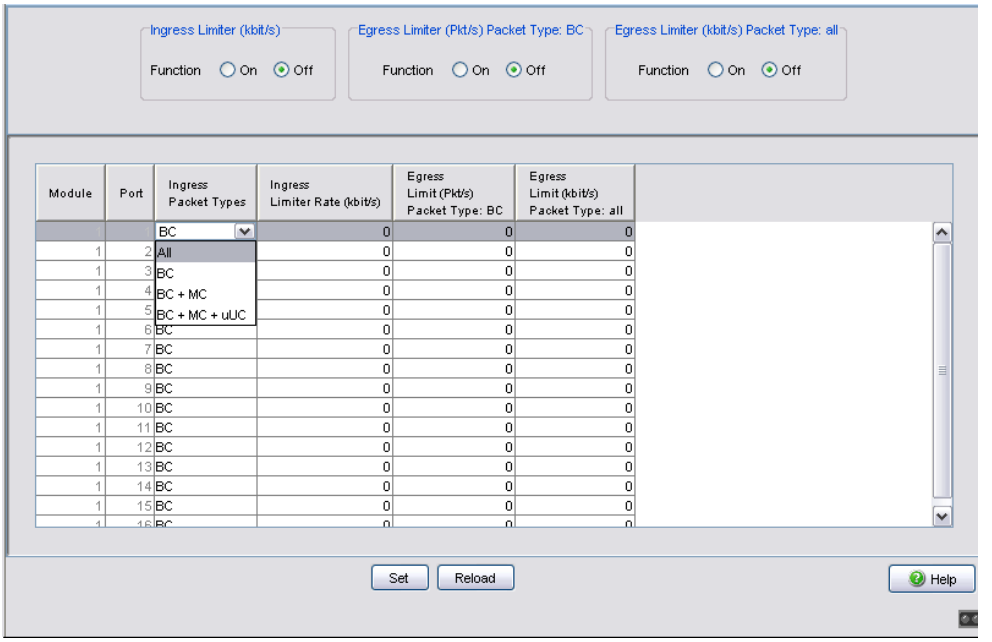


Figure 26: Rate Limiter Dialog

4.3.2 Rate Limiter Settings (PowerMICE and MACH 4000)

- "Ingress Limiter (kbit/s)" allows you to enable or disable the ingress limiter function for all ports and to select the ingress limitation on all ports (either broadcast packets only or broadcast packets and Multicast packets).
- "Egress Limiter (Pkt/s)" allows you to enable or disable the egress limiter function for broadcasts on all ports.

Setting options per port:

- Ingress Limiter Rate for the packet types selected in the Ingress Limiter frame:
  - = 0, no ingress limit at this port.
  - > 0, maximum incoming traffic rate in kbit/s that is allowed to be sent at this port.
- Egress Limiter for broadcast packets:
  - = 0, no rate limit for outbound broadcast packets at this port.
  - > 0, maximum number of outgoing broadcasts per second sent at this port.

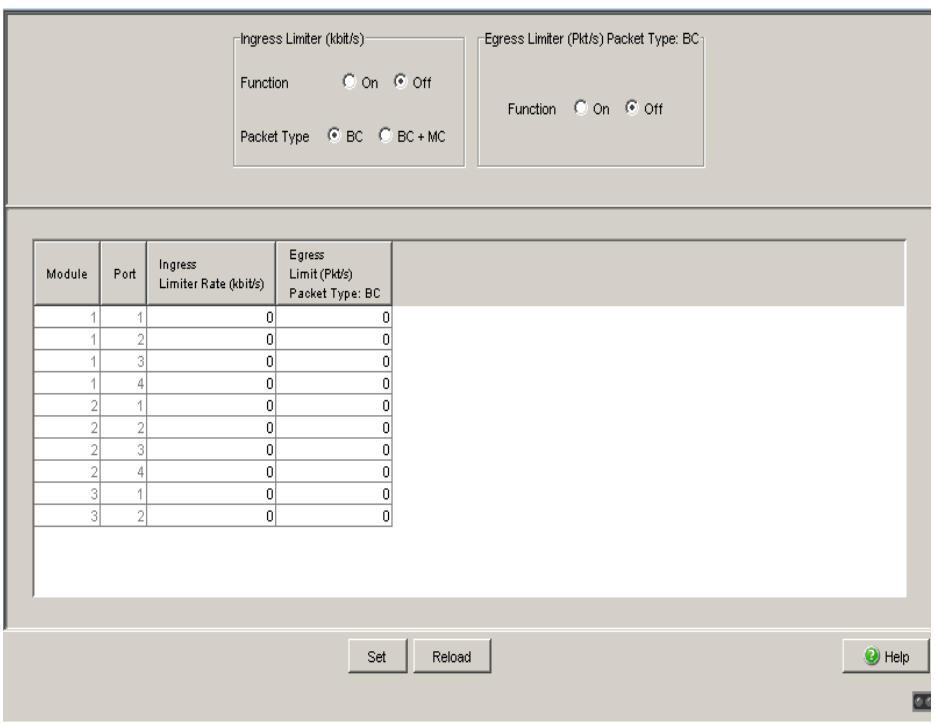


Figure 27: Rate Limiter dialog

4.4 Multicasts

4.4.1 IGMP (Internet Group Management Protocol)

With this dialog you can
- activate/deactivate the IGMP Snooping protocol,
- configure the IGMP Snooping protocol globally and per port.

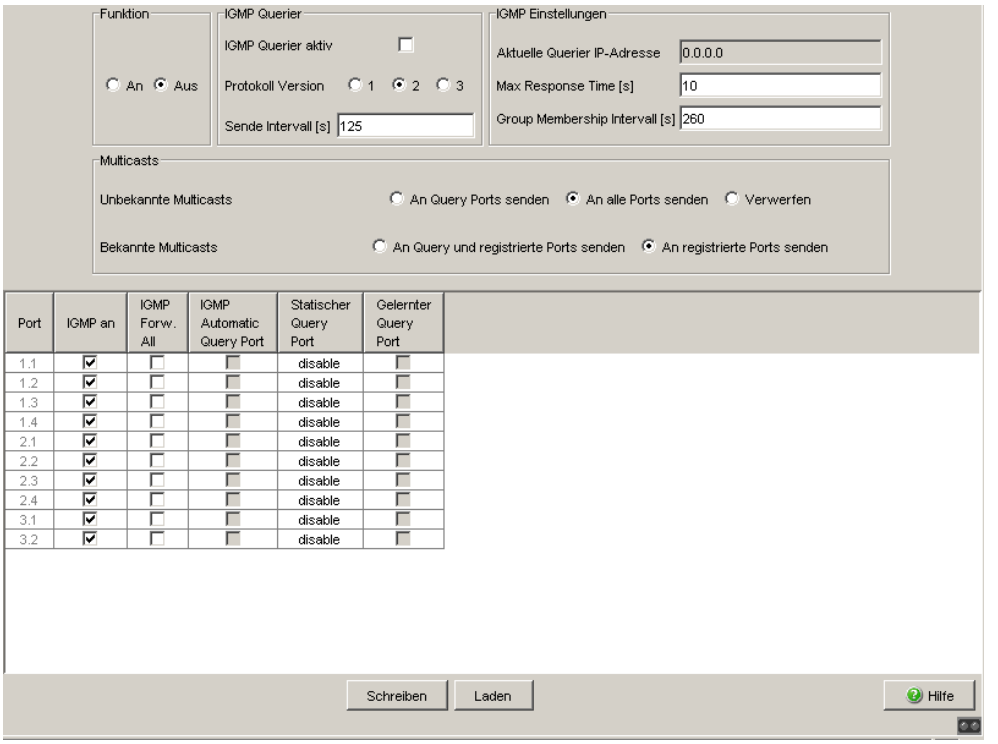


Figure 28: IGMP Snooping dialog

Operation
In this frame you can:

- activate/deactivate the IGMP Snooping protocol.

Parameter	Meaning	Value range	Default setting
Function	Activate/deactivate IGMP Snooping globally for the device. If IGMP Snooping is switched off: ▶ the device does not evaluate Query and Report packets received, and ▶ it sends (floods) received data packets with a Multicast address as the destination address to all ports.	`On`, `Off`	`Off`

Table 32: IGMP Snooping, global function

IGMP Querier and IGMP Settings

With these frames you can enter global settings for the IGMP settings and the IGMP Querier function.

Prerequisite: The IGMP Snooping function is activated globally.

Parameter	Meaning	Value range	Default setting
IGMP Querier			
IGMP Querier enabled	Switch query function on/off	on/off	off
Protocol Version	Select IGMP version 1, 2 or 3.	1, 2, 3	2
Send Interval	Enter the interval at which the switch sends query packets. All IGMP-capable terminal devices respond to a query with a report message, thus generating a network load.	2-3599 s[a]	125 s
IGMP settings			
Current querier IP address	Display the IP address of the router/ switch that contains the query function.		
Max. Response Time	Enter the time within which the Multicast group members respond to a query. The Multicast group members select random values within the response time for their response, so that all the Multicast group members do not respond to the query at the same time.	Protocol Version - 1,2: 1-25 s[a] - 3: 1-3598 s[a]	10 s
Group Membership Interval	Enter the period for which a dynamic Multicast group remains entered in the device if it does not receive any report messages.	3-3600 s[a]	260 s

Table 33: IGMP Querier and IGMP settings

a.) Note the connection between the parameters Max. Response Time, Send Interval and Group Membership Interval, (see table 34)

The parameters
– Max. Response Time,
– Send Interval and
– Group Membership Interval
have a relationship to each other:

Max. Response Time < Send Interval < Group Membership Interval.

If you enter values that contradict this relationship, the device then replaces these values with a default value or with the last valid values.

Parameter	Protocol Version	Value range	Default setting
Max. Response Time,	1, 2 3	1-25 seconds 1-3,598 seconds	10 seconds
Send Interval	1, 2, 3	2-3,599 seconds	125 seconds
Group Membership Interval	1, 2, 3	3-3,600 seconds	260 seconds

Table 34: Value range for
- Max. Response Time
- Send Interval
- Group Membership Interval

For “Send Interval” and “Max. Response Time”,
– select a large value if you want to reduce the load on your network and can accept the resulting longer switching times,
– select a small value if you require short switching times and can accept the resulting network load.

Multicasts

In this frame you specify how the device transmits packets with
- unknown MAC/IP Multicast address not learned with IGMP Snooping
- known MAC/IP Multicast address learned with IGMP Snooping.

Prerequisite: The IGMP Snooping function is activated globally.

Parameter	Meaning	Value range	Default setting
Unknown Multicasts			
	▶ Send to Query Ports: The device sends the packets with an unknown MAC/IP Multicast address to all query ports. ▶ Send to All Ports: The device sends the packets with an unknown MAC/IP Multicast address to all ports. ▶ Discard: The device discards all packets with an unknown MAC/IP Multicast address.	Send to Query Ports, Send to All Ports, Discard	Send to All Ports
Known Multicasts			
	▶ Send to query and registered ports: The device sends the packets with a known MAC/IP Multicast address to all query ports and to registered ports. The advantage of this is that it works in most applications without any additional configuration. Application: “Flood and Prune” routing in PIM-DM. ▶ Send to registered ports: The device sends the packets with a known MAC/IP Multicast address to registered ports. The advantage of this setting is that it uses the available bandwidth optimally through direct distribution. It requires additional port settings. Application: Routing protocol PIM-SM.	Send to query and registered ports, send to registered ports	Send to registered ports

Table 35: Known and unknown Multicasts

Note: The way in which unlearned Multicast addresses are handled also applies to the reserved addresses from the “Local Network Control Block” (224.0.0.0 - 224.0.0.255). This can have an effect on higher-level routing protocols.

Settings per Port (Table)

With this configuration table you can enter port-related IGMP settings.

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies.	-	-
IGMP Snooping on	Switch IGMP on/off for each port. Switching IGMP off at a port prevents registration for this port. Prerequisite: In the `Switching:Multicasts:IGMP` dialog, IGMP is enabled.	`on`, `off`	`on`
IGMP Forward All	Switch the IGMP Snooping function “Forward All” on/off. With the `IGMP Forward All` setting, the device sends to this port all data packets with a Multicast address in the destination address field. Prerequisite: In the `Switching:Multicasts:IGMP` dialog, IGMP is enabled. **Note:** If a number of routers are connected to a subnetwork, you must use IGMP version 1 so that all the routers receive all the IGMP reports. **Note:** If you use IGMP version 1 in a subnetwork, then you must also use IGMP version 1 in the entire network.	`on`, `off`	off
IGMP Automatic Query Port	Displays which ports the device has learned as query ports if `automatic` is selected in “Static Query Port”. Prerequisite: The IGMP Snooping function is activated globally.	`yes`, `no`	-
Static Query Port	The device sends IGMP report messages to the ports at which it receives IGMP queries (default setting). This column allows you to also send IGMP report messages to: other selected ports (enable) or connected Hirschmann devices (automatic). Prerequisite: The IGMP Snooping function is activated globally.	`enable`, `disable`, `automatic`	`disable`
Learned Query Port	Shows at which ports the device has received IGMP queries if “disable” is selected in “Static Query Port”. Prerequisite: In the `Switching:Multicasts:IGMP` dialog, IGMP is enabled.	`yes`, `no`	-

Table 36: Settings per port

Note: If the device is incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

- Switch on the IGMP Snooping on the ring ports and globally, and
- activate “IGMP Forward All” per port on the ring ports.

4.4.2 GMRP (GARP Multicast Registration Protocol)

With this dialog you can:

- activate/deactivate the GMRP function globally,
- configure the GMRP for each Port.

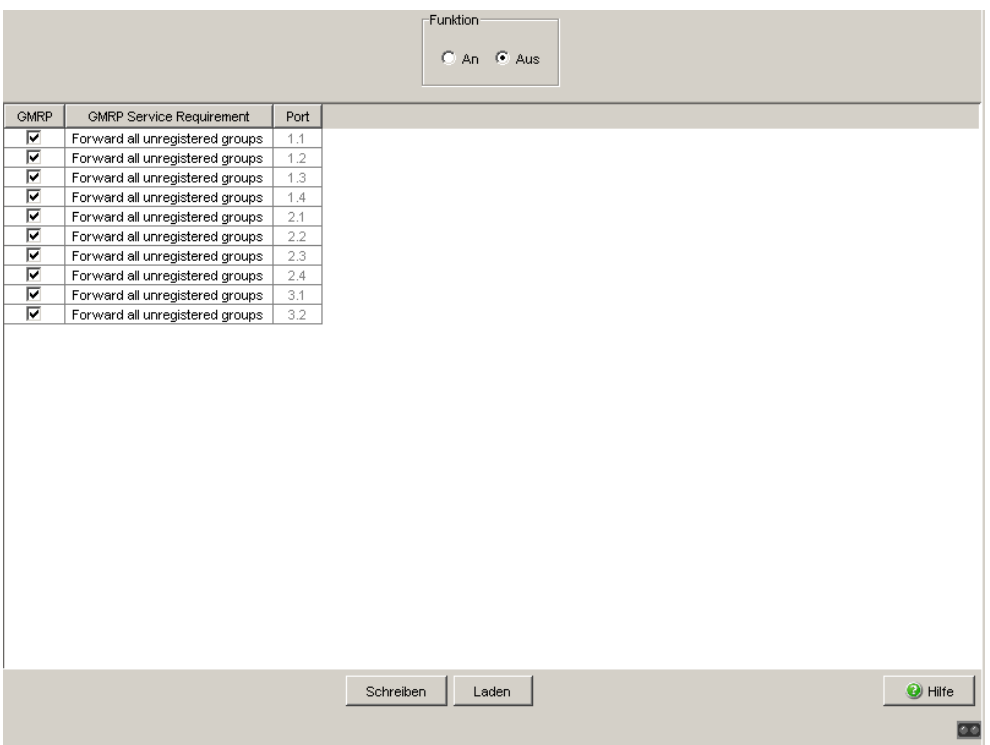


Figure 29: Multicasts dialog

Operation

In this frame you can:

- activate/deactivate the GMRP function globally.

Parameter	Meaning	Default setting
GMRP	Activate GMRP globally for the entire device. If GMRP is switched off: ▶ the device does not generate any GMRP packets, ▶ does not evaluate any GMRP packets received, and ▶ sends (floods) received data packets to all ports. The device is transparent for received GMRP packets, regardless of the GMRP setting.	`Off`

Table 37: Global setting

Settings per Port (Table)

With this configuration table you can enter port-related GMRP settings.

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies.	-	-
GMRP	Switch GMRP on/off for each port. When you disable GMRP at a port, no registrations can be made for this port, and GMRP packets cannot be forwarded at this port. Prerequisite: In the `Switching:Multicasts:GMRP` dialog, GMRP is enabled.	`On`, `Off`	`On`
GMRP Service Requirement	Devices that do not support GMRP can be integrated into the Multicast addressing by means of – a static filter address entry on the connecting port. – selecting “Forward all groups”. The device enters ports with the selection “Forward all groups” in all Multicast filter entries learned via GMRP. Prerequisite: In the `Switching:Multicasts:GMRP` dialog, GMRP is enabled.	`Forward all groups`, `Forward all unregistered groups`	`Forward all unregistered groups`

Table 38: GMRP settings per port

Note: If the device is incorporated into a HIPER-Ring, you can use the following settings to quickly reconfigure the network for data packets with registered Multicast destination addresses after the ring is switched:

- Activate GMRP on the ring ports and globally, and
- activate “Forward all groups” on the ring ports.

4.5 VLAN

VLAN contains dialogs and attributes for configuring and monitoring the VLAN function in accordance with the IEEE 802.1Q standard.

4.5.1 VLAN Global

With this dialog you can:

- display VLAN parameters
- activate/deactivate the VLAN 0 transparent mode
- activate/deactivate GVRP
- configure and display the learning mode
- reset the VLAN settings of the device to the original defaults.

Parameter	Meaning
Max. VLAN ID	Displays the largest possible VLAN ID (see on page 115 “VLAN Static“).
Max. supported VLANs	Displays the maximum number of VLANs the device supports (see on page 115 “VLAN Static“).
Number of VLANs	Displays the number of configured VLANs (see on page 115 “VLAN Static“).

Table 39: VLAN display

Note: The device provides the VLAN with the ID 1. The VLAN with ID 1 is always present.

Parameter	Meaning	Value range	Default setting
VLAN 0 Transparent Mode	When the VLAN 0 Transparent Mode is activated, the device accepts a VLAN ID of 0 in the packet when it receives it, regardless of the setting for the port VLAN ID in the dialog (see on page 117 “VLAN Port“). Activate “VLAN 0 Transparent Mode” to transmit packets with a priority TAG without VLAN membership, i.e. with a VLAN ID of 0.	`On`, `Off`	`Off`
GVRP	Activate “GVRP” to ensure the distribution of VLAN information to the neighboring devices via GVRP data packets.	`On`, `Off`	`Off`

Table 40: VLAN settings

Note: If you are using the GOOSE protocol in accordance with IEC61850-8-1, you activate the “VLAN 0 transparent mode”. Thus the prioritizing information remains in the data packet in accordance with IEEE802.1D/p even when the device forwards the data packet.
This also applies to other protocols that use this prioritizing in accordance with IEEE802.1D/p but that do not require any VLANs in accordance with IEEE802.1Q.

Note: When using the “Transparent Mode” in this way, note the following:

- For RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
  In “Transparent mode”, the devices ignore the port VLAN ID set. Set the VLAN membership of the ports of VLAN 1 to `U` (Untagged) or `T` (Tagged), (see on page 115 “VLAN Static“).
- For PowerMICE, MACH 104, MACH 1040 and MACH 4000:
  In “Transparent mode”, the devices ignore the VLAN tags and the priority tag on reception. Set the ports’ VLAN membership for all VLANs to "`U`“ (Untagged).
- For MACH 4002-24/48G:
  In “Transparent mode”, the devices ignore the VLAN tags but evaluate the priority tag. Set the ports’ VLAN membership for all VLANs to "`U`“ (Untagged).

Parameter	Meaning	Value range	Default setting
Mode	VLAN mode selection. **"Independent VLAN“** subdivides the forwarding database (see on page 94 “Filters for MAC addresses“) virtually into one independent forwarding database per VLAN. The device cannot assign data packets with a destination address in another VLAN, and so floods it to all ports of the VLAN. **Application area:** Setting up identical networks that use the same MAC addresses. **"Shared VLAN“** uses the same forwarding database for all VLANs (see on page 94 “Filters for MAC addresses“). The device cannot assign data packets with a destination address in another VLAN, and so only forwards them to the destination port if the receiving port is also a member of the VLAN group of the destination port. **Application area:** In the case of overlapping groups, the device can distribute directly across VLANs, as long as the ports involved belong to a VLAN that can be reached. Changes to the mode are only taken over after a warm start (see on page 38 “Restart“) is performed on the device, and the changes are then displayed in the line below under “Status”.	Independent VLAN, Shared VLAN	Independent VLAN
Status	Displays the current status. After a warm start (see on page 38 “Restart“) on the device, the device take the setting for the “Mode” into the status line.	Independent VLAN, Shared VLAN	

Table 41: Settings and displays in the “Learning” frame

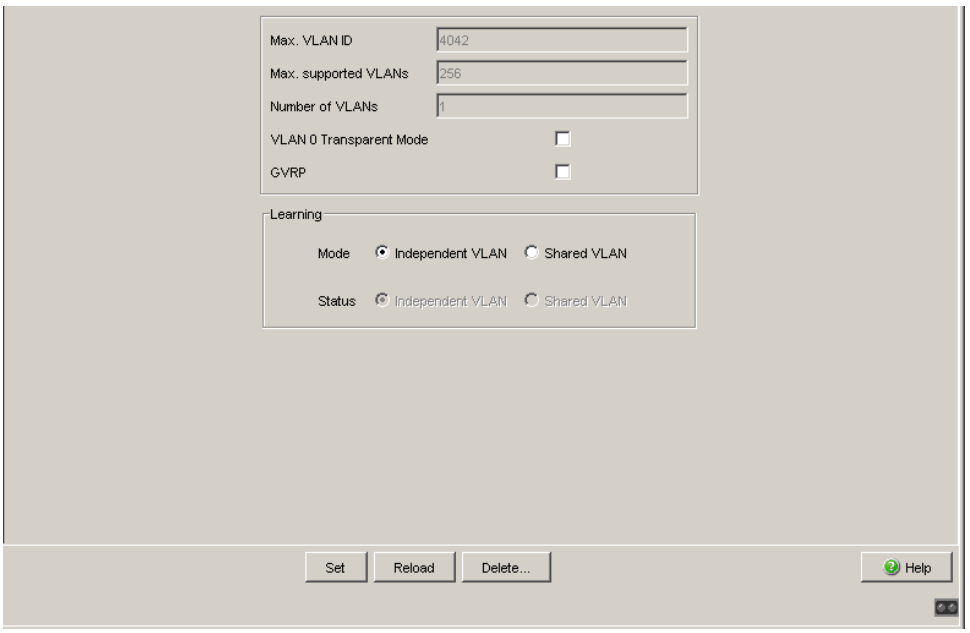


Figure 30: VLAN Global dialog

4.5.2 Current VLAN

With this dialog you can:

- display VLAN parameters

The Current VLAN table shows all
– manually configured VLANs
– VLANs configured via redundancy mechanisms
– VLANs configured via GVRP
The Current VLAN table is only used for information purposes. You can make changes to the entries in the `VLAN:Static` dialog.

Note: Ports not displayed are participants in the link aggregation. You can assign these ports to a VLAN using the port assigned to the link aggregation in module 8 (display 8.X).

Parameter	Meaning	Value range
VLAN ID	Displays the ID of the VLAN.	
Status	Displays the VLAN status.	`other`: This entry solely appears for VLAN 1. The system provides VLAN 1. VLAN 1 is always present. `permanent`: A static entry made by you. This entry is kept when the device is restarted. dynamic: This VLAN was created dynamically via GVRP.
Time created	Operating time (see "System Data") at which the VLAN was created.	
Ports x.x	VLAN membership of the relevant port and handling of the VLAN tag.	– Currently not a member `T` Member of VLAN; send data packets with tag. `U` Member of the VLAN; send data packets without tag (untagged). `F` Membership forbidden, so no entry possible via GVRP either.

Table 42: Current VLAN

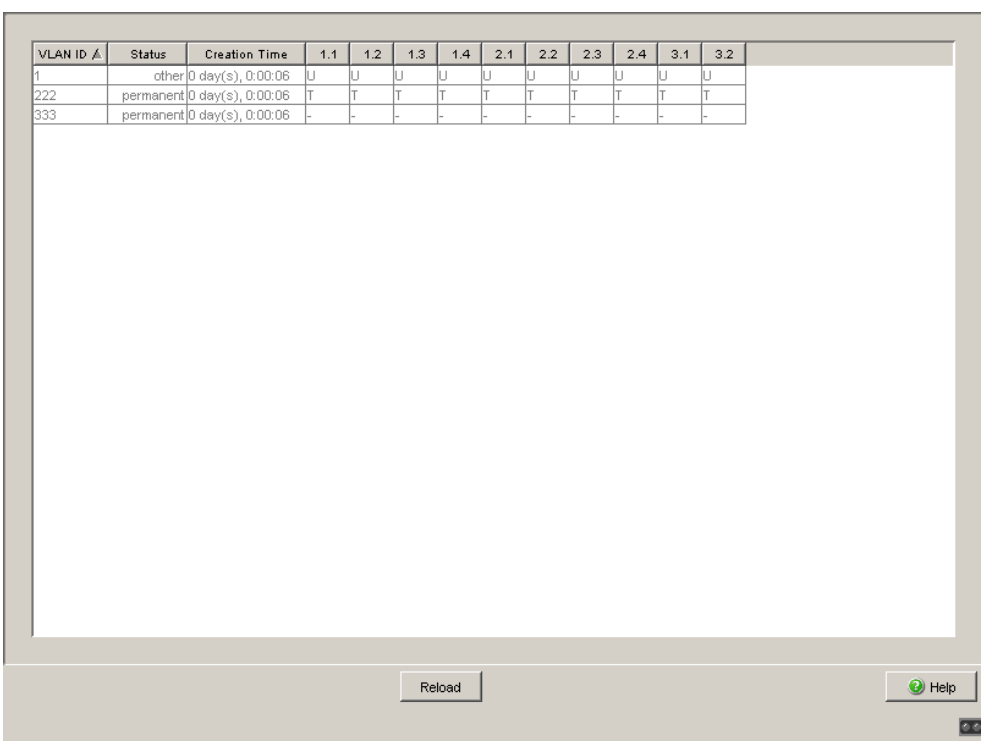


Figure 31: Current VLAN dialog

4.5.3 VLAN Static

With this dialog you can:

- Create VLANs
- Assign names to VLANs
- Assign ports to VLANs and configure them
- Delete VLANs

Parameter	Meaning	Possible Values	Default Setting
VLAN ID	Displays the ID of up to 255 VLANs that are simultaneously possible. (Up to 256 VLANs possible simultaneously for Power MICE, MACH 104, MACH 1040, MACH 4000.)	1-4.042 (1-3,966 for PowerMICE, MACH 104, MACH 1040, MACH 4000)	
Name	Enter the name of your choice for this VLAN.	Maximum 32 characters	VLAN 1: default
Status	Displays the VLAN status.	`active`: Entry is activated `notInService`: Entry is deactivated	`active`
Ports x.x	Select the membership of the ports to the VLANs.	`-`: currently not a member (GVRP allowed). `T`: Member of the VLAN; send data packets with tag (tagged). `U`: Member of the VLAN; send data packets without tag (untagged). `F`: Membership forbidden, so no entry possible via GVRP either.	VLAN 1: `U`, new VLANs: `-`

Table 43: VLAN Static dialog

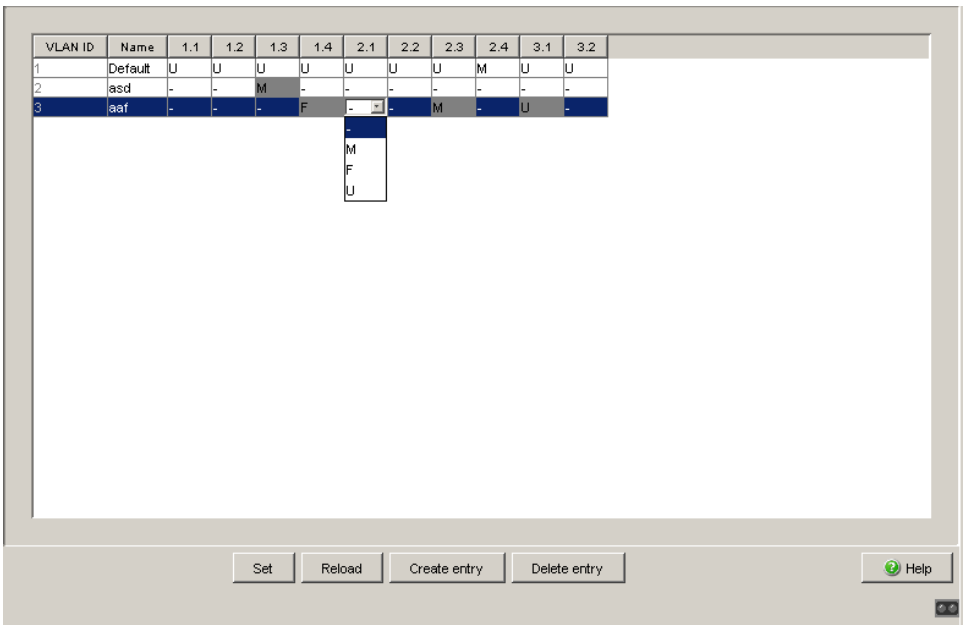


Figure 32: VLAN Static Dialog

Note: When configuring the VLAN, the management station must maintain access to the device after the VLAN configuration is saved.
You achieve this by connecting the management station to a port with the VLAN ID 1. The device transmits the data of the management station in VLAN 1.

Note: The device automatically creates VLANs for MRP rings. The MRP ring function prevents the deletion of these VLANs.

Note: Note the tagging settings for ports (see table 44) that are part of a redundant Ring or the Ring/network coupling.

Redundancy	VLAN membership
HIPER-Ring	VLAN 1 U
MRP-Ring	any
Fast HIPER-Ring	any
Ring/Network coupling	VLAN 1 U

Table 44: Required VLAN settings of ports that are part of redundant Rings or Ring/ Network coupling.

Note: In a redundant ring with VLANs, you should only operate devices whose software version supports VLANs:

- RS2 xx/xx (from rel. 7.00)
- RS2-16M
- RS20, RS30, RS40 (with software variants L2E, L2P)
- MICE (from rel. 3.0)
- PowerMICE
- MS20, MS30
- RSR20, RSR30
- MACH 100
- MACH 1000
- MACH 4000
- MACH 3000 (from Rel. 3.3),
- OCTOPUS

4.5.4 VLAN Port

With this dialog you can:

- assign ports to VLANs
- define the Acceptable Frame Type
- activate/deactivate Ingress Filtering
- activate/deactivate GVRP

Parameter	Meaning	Possible Values	Default Setting
Module	Module of the device on which the port is located.		
Port	Port to which this entry applies.		
Port VLAN ID	Specifies the VLAN to which the port assigns a received untagged data packet.	All allowed VLAN IDs	1
Acceptable Frame Types	Specifies whether the port may also receive untagged data packets.	- `admitAll` - `admitOnlyVlanTagged`	`admitAll`
Ingress Filtering	Specifies whether the port evaluates the received tags.	`on`, `off`	`off`
GVRP	- on: The device sends and receives GVRP data packets. The device exchanges VLAN configuration data with other devices. - off: The device does not send or receive GVRP data packets. The device does not exchange VLAN configuration data with other devices.	`on`, `off`	`off`

Table 45: VLAN Port dialog

Note: If you selected `admitOnlyVlanTagged` under “Acceptable Frame Types” and GVRP is active, you assign the value 0 to the VLAN ID in `Basic Settings:Network`.

Note: Note the following:

- HIPER-Ring
  Select the port VLAN ID 1 for the ring ports and deactivate “`Ingress Filtering`”.
- MRP-Ring
  - If the MRP-Ring configuration (see on page 145 “Configuring the MRP-Ring“) is not assigned to a VLAN, select the port VLAN ID 1.
  - If the MRP-Ring configuration (see on page 145 “Configuring the MRP-Ring“) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.
- Fast HIPER-Ring (RSR20, RSR30 and MACH 1000)

– If the Fast HIPER-Ring configuration (see on page 148 “Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)“) is not assigned to a VLAN, select the port VLAN ID 1.
– If the Fast HIPER-Ring configuration (see on page 148 “Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)“) is assigned to a VLAN, the device automatically performs the VLAN configuration for this port.

▶ Network/Ring coupling
Select the VLAN ID 1 for the coupling and partner coupling ports and deactivate “`Ingress Filtering`”.

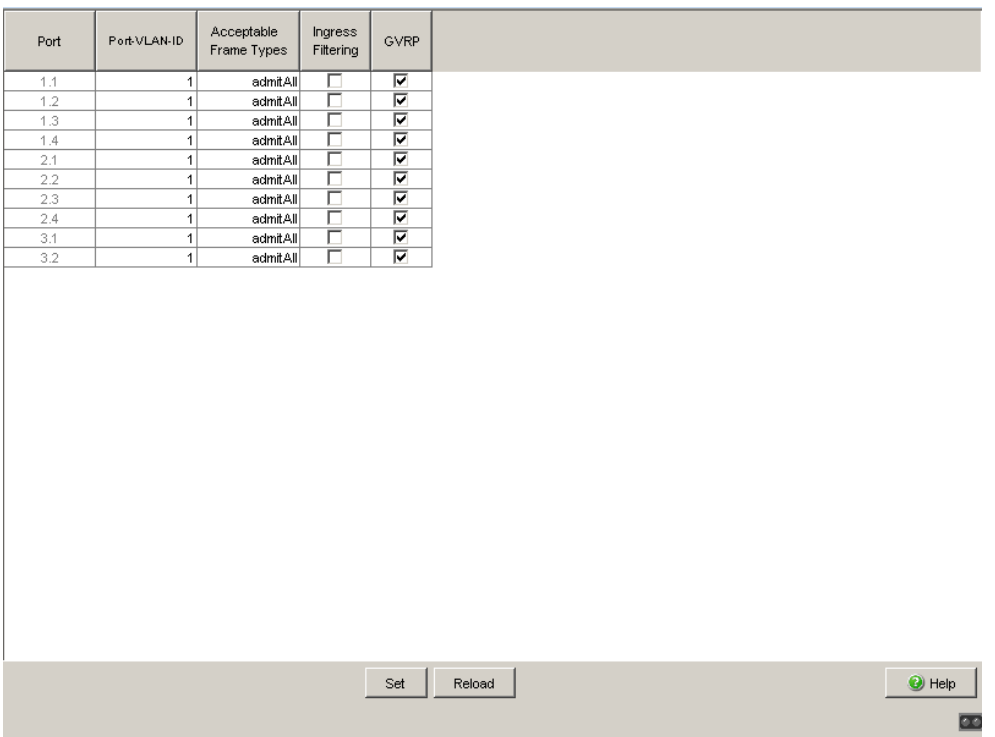


Figure 33: VLAN Port dialog

5 QoS/Priority

The device enables you to set

- how it evaluates the QoS/prioritizing information of incoming data packets:
  - VLAN priority based on IEEE 802.1Q/ 802.1D (Layer 2)
  - Type of Service (ToS) or DiffServ (DSCP) for IP packets (Layer 3)
- which QoS/prioritizing information it writes to outgoing data packets (e.g. priority for management packets, port priority).

The QoS/Priority menu contains the dialogs, displays and tables for configuring the QoS/priority settings:

- Global
- Port configuration
- IEEE 802.1D/p mapping
- IP DSCP mapping

5.1 Global

With this dialog you can:

- enter the VLAN priority for management packets in the range 0 to 7 (default setting: 0).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
  Note the assignment of the VLAN priority to the traffic class (see table 50).
- enter the IP-DSCP value for management packets in the range 0 to 63 (default setting: 0 (be/cs0)).
  In order for you to have full access to the management of the device, even when there is a high network load, the device enables you to prioritize management packets.
  In prioritizing management packets (SNMP, Telnet, etc.), the device sends the management packets with priority information.
  Note the assignment of the IP-DSCP value to the traffic class (see table 51).

  Note: Certain DSCP values have DSCP names, such as be/cs0 to cs7 (class selector) or af11 to af43 (assured forwarding) and ef (expedited forwarding).

- display the maximum number of queues possible per port.
  The device supports 4 (8 for MACH 4000, MACH 104, MACH 1040 and PowerMICE) priority queues (traffic classes in compliance with IEEE 802.1D).
- select the trust mode globally (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS). You use this to specify how the device handles received data packets that contain priority information.
  - “untrusted”:
    The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.

- “trustDot1p”:
  The device prioritizes received packets that contain VLAN tag information according to this information (assigning them to a traffic class - see “802.1D/p mapping“).
  The device prioritizes received packets that do not contain any tag information (assigning them to a traffic class - see “Entering the port priority“) according to the port priority of the receiving port .
- “trustIpDscp”:
  The device prioritizes received IP packets (assigning them to a traffic class - see “IP DSCP mapping“) according to their DSCP value.
  The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see “Entering the port priority“) according to the port priority of the receiving port .
  For received IP packets:
  The device also performs VLAN priority remarking.
  In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag (see on page 115 “VLAN Static“).
  Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with table 46.
  Example: A received IP packet with a DSCP value of 32 (cs4) is assigned to traffic class 2 (default setting). The packet was received at a port with port priority 2. Based on table 46, the VLAN priority is set to 4.

Traffic class	New VLAN priority when receiving port has an even port priority	New VLAN priority when receiving port has an odd port priority
0	0	1
1	2	3
2	4	5
3	6	7

Table 46: VLAN priority remarking

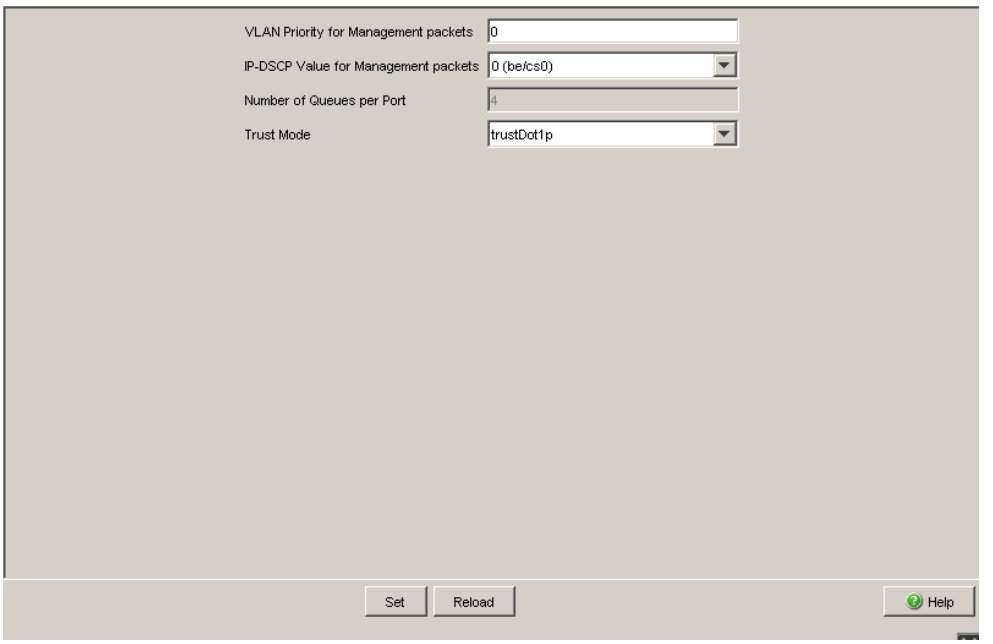


Figure 34: Global dialog (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS)

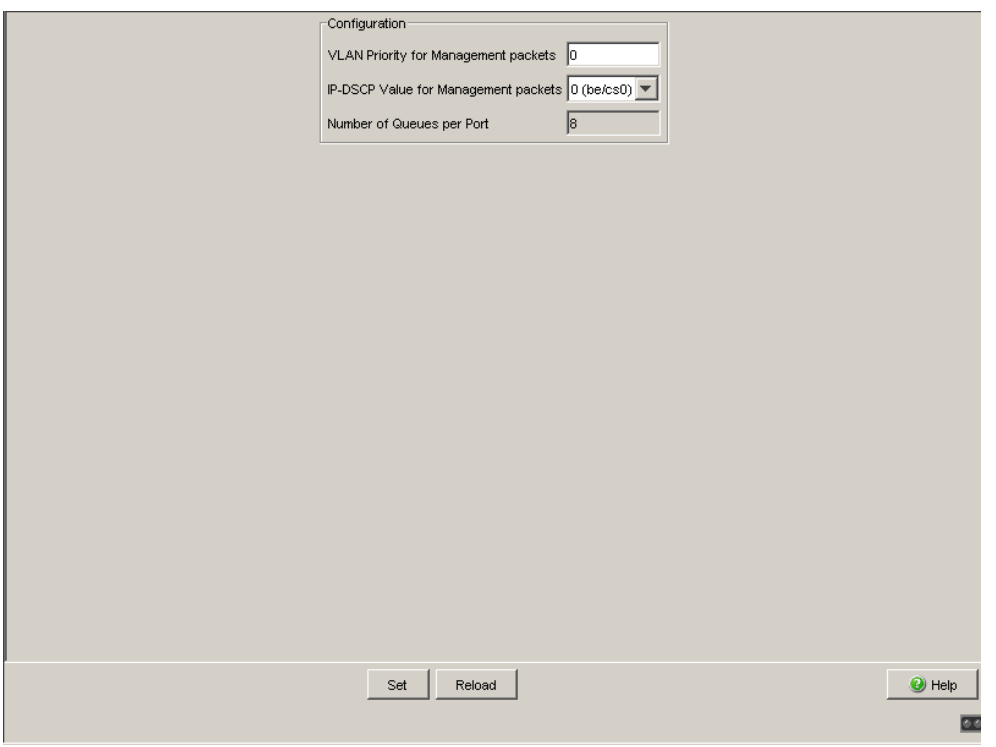


Figure 35: Global dialog (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

5.2 Port Configuration

This dialog allows you to configure the ports. You can:
- assign a port priority to a port,
- select the trust mode for a port (PowerMICE, MACH 104, MACH 1040 and MACH 4000),
- display the untrusted traffic class (PowerMICE, MACH 104, MACH 1040 and MACH 4000),

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port priority	Enter the port priority.

Table 47: Port configuration table for RS20/RS30/RS40, MS20/MS30, RSR20/ RSR30, MACH 1000 and OCTOPUS

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Port priority	Enter the port priority.
Trust mode	Select the trust mode.
Untrusted traffic class	Display the traffic class used in the “untrusted” trust mode.

Table 48: Port configuration table for PowerMICE, MACH 104, MACH 1040 and MACH 4000

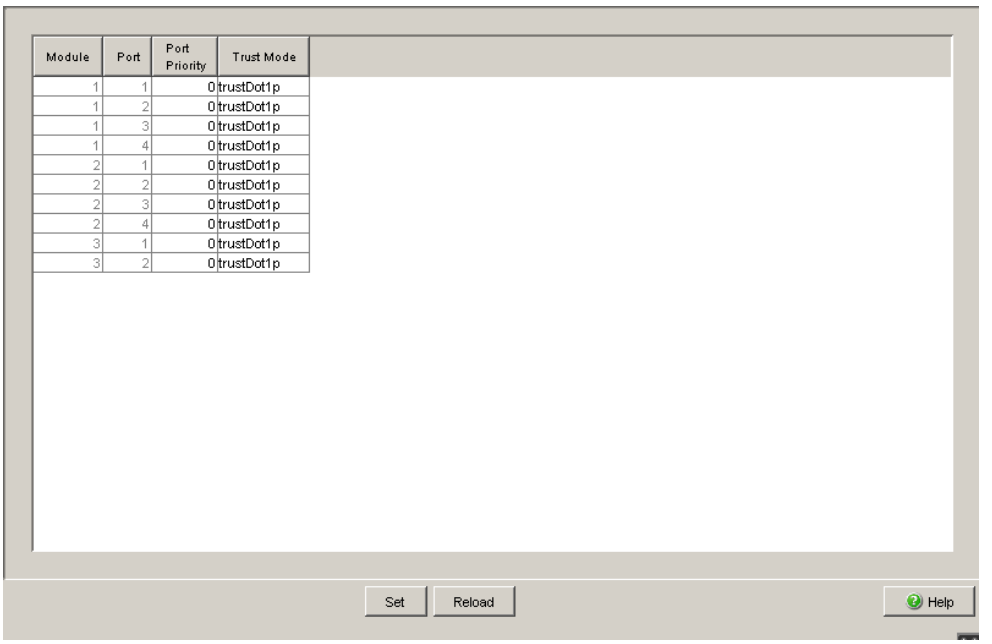


Figure 36: Port configuration dialog for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 and OCTOPUS

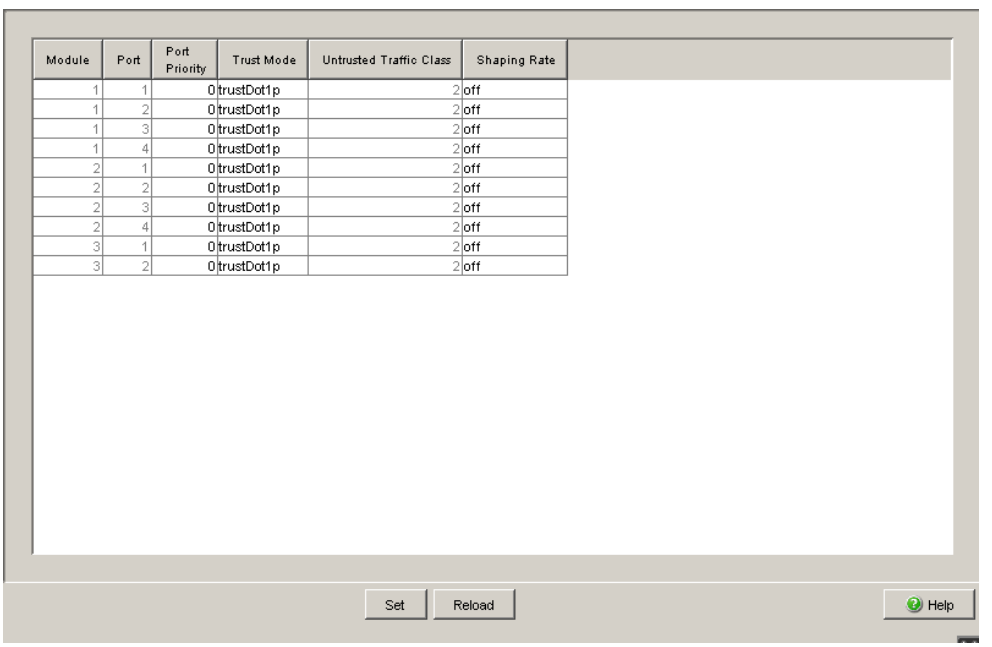


Figure 37: Port configuration dialog for PowerMICE, MACH 104, MACH 1040 and MACH 4000

5.2.1 Entering the port priority

☐ RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS:
Double-click a cell in the “Port priority” column and enter the priority (0-7). According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class (see table 49).
Prerequisite:
setting in the `Global:Trust Mode dialog: untrusted` (see on page 122 “Global“) or
setting in the `Global:Trust Mode dialog:trustDot1p`(see on page 122 “Global“) and the data packets do not contain a VLAN tag or
setting in `Global:Trust Mode dialog: trustIpDscp`(see on page 122 “Global“) and the data packets are not IP packets.

☐ Power MICE, MACH 104, MACH 1040 and MACH 4000:
Double-click a cell in the “Port priority” column and enter the priority (0-7). According to the priority entered, the device assigns the data packets that it receives at this port to a traffic class (see table 49).
Prerequisite:
setting in the `Trust Mode column: untrusted` or
setting in the `Trust Mode column: trustDot1p` and the data packets do not contain a VLAN tag or
setting in `Trust Mode column: trustIpDscp` and the data packets are not IP packets.

Port priority	Traffic class for RS20/RS30/ RS40, MS20/MS30, RSR20/RSR30, MACH 100 MACH 1000, OCTOPUS (default setting)	Traffic Class for MACH 4000, MACH 104, MACH 1040 and PowerMICE (default setting)	IEEE 802.1D traffic type
0	1	2	Best effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent effort (business critical)
4	2	4	Controlled load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter
6	3	6	Voice, < 10 ms of latency and jitter
7	3	7	Network control reserved traffic

Table 49: Assigning the port priority to the traffic classes

5.2.2 Selecting the trust mode (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

The device provides 3 options for selecting how it handles received data packets that contain priority information. Click once on a cell in the “Trust mode” column to select one of the 3 options:

- “untrusted”
  The device ignores the priority information in the packet and always assigns the packets the port priority of the receiving port.
- “trustDot1p”
  The device prioritizes received packets that contain VLAN tag information (assigning them to a traffic class - see “802.1D/p mapping“) in accordance with this information.
  The device prioritizes received packets that do not contain any VLAN tag information (assigning them to a traffic class - see “Entering the port priority“) according to the port priority of the receiving port .

- “trustIpDscp”:
  The device prioritizes received IP packets (assigning them to a traffic class - see “IP DSCP mapping“) according to their DSCP value.
  The device prioritizes received packets that are not IP packets (assigning them to a traffic class - see “Entering the port priority“) according to the port priority of the receiving port .
  For received IP packets:
  The device also performs VLAN priority remarking.
  In VLAN priority remarking, the device modifies the VLAN priority of the IP packets if the packets are to be sent with a VLAN tag (see on page 115 “VLAN Static“).

  Based on the traffic class to which the IP packet was assigned (see above), the device assigns the new VLAN priority to the IP packet in accordance with table 50.
  Example: A received IP packet with a DSCP value of 16 (cs2) is assigned traffic class 1 (default setting). The packet is now assigned VLAN priority 2 in accordance with table 50.

5.2.3 Displaying the untrusted traffic class (PowerMICE, MACH 104, MACH 1040 and MACH 4000)

“Untrusted traffic class” shows you the traffic class that is used in the “untrusted” trust mode. When you change the port priority (see on page 127 “Entering the port priority“), the untrusted traffic class also changes (see table 49).

5.3 802.1D/p mapping

The 802.1D/p mapping dialog allows you to assign a traffic class to every VLAN priority.

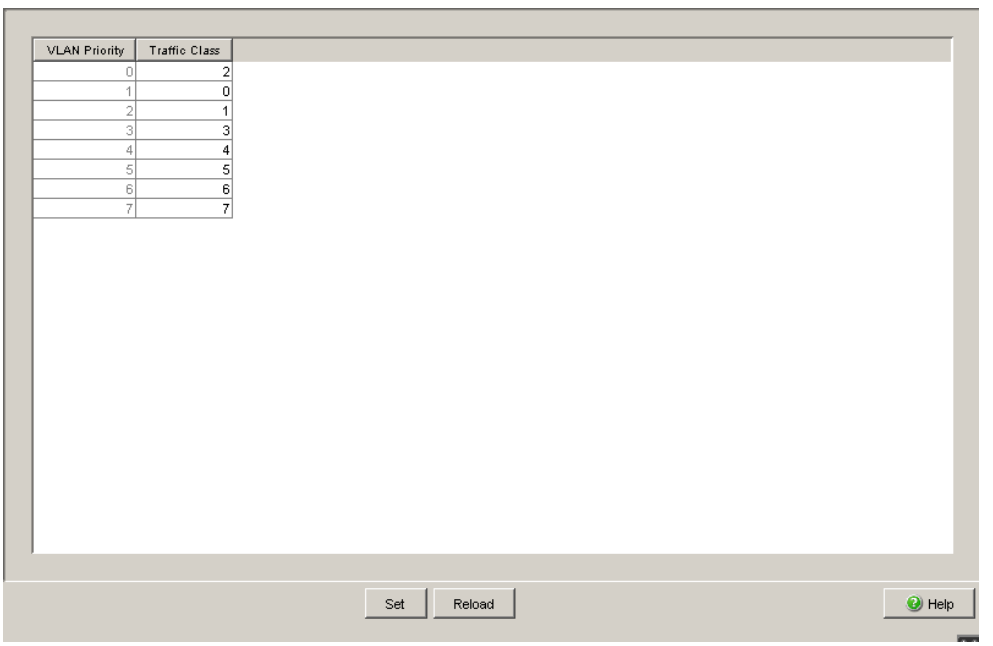


Figure 38: 802.1D/p Mapping dialog

☐ Enter following desired values in the Traffic Class field for every VLAN priority:

- between 0 and 3 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS
- between 0 and 7 for MACH 4000, MACH 104, MACH 1040 and PowerMICE.

VLAN priority	Traffic class for RS20/RS30/ RS40, MS20/ MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (default setting)	Traffic class for MACH 4000, MACH 104, MACH 1040 and PowerMICE (default setting)	IEEE 802.1D traffic type
0	1	2	Best effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent effort (business critical)
4	2	4	Controlled load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter
6	3	6	Voice, < 10 ms of latency and jitter
7	3	7	Network control reserved traffic

Table 50: Assigning the VLAN priority to the traffic classes

Note: Network protocols and redundancy mechanisms use the highest traffic classes 3 (RS20/30/40, MS20/30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS) or 7 (PowerMICE, MACH 104, MACH 1040, MACH 4000). Therefore, select other traffic classes for application data.

5.4 IP DSCP mapping

The IP DSCP mapping table allows you to assign a traffic class to every DSCP value.

☐ Enter the desired value from in the Traffic Class field for every DSCP value (0-63)

- between 0 and 3 for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 and OCTOPUS
- between 0 and 7 for MACH 4000, MACH 104, MACH 1040 and PowerMICE.

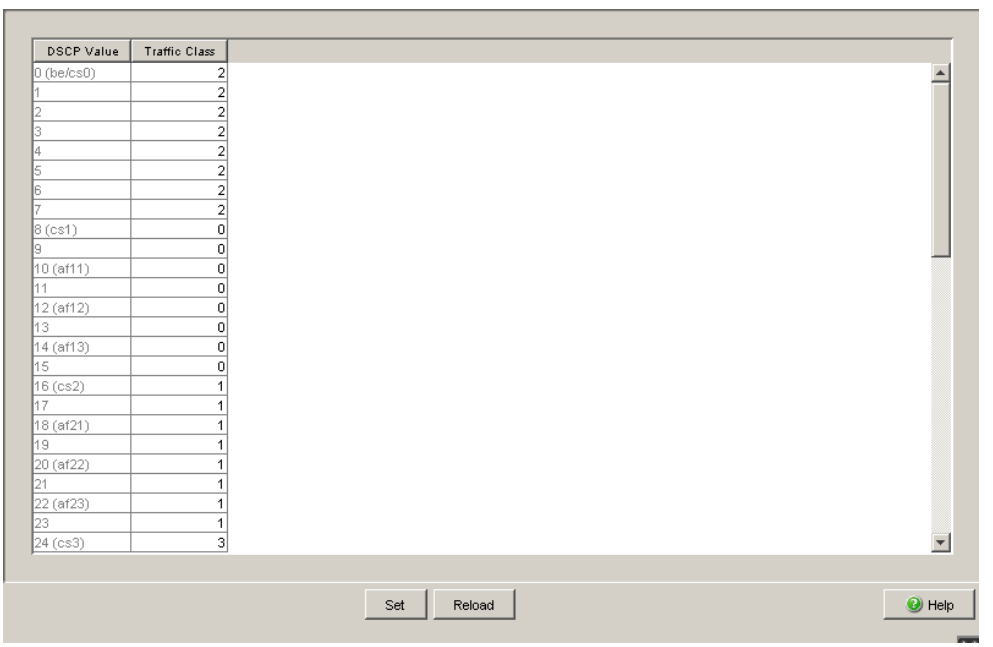


Figure 39: IP DSCP mapping table

The different DSCP values get the device to employ a different forwarding behavior, namely Per-Hop Behavior (PHB).
PHB classes:

- Class Selector (CS0-CS7): For reasons of compatibility to TOS/IP Precedence
- Expedited Forwarding (EF): Premium service.
  Reduced delay, jitter + packet loss (RFC 2598)
- Assured Forwarding (AF): Provides a differentiated schema for handling different data traffic (RFC 2597).
- Default Forwarding/Best Effort: No particular prioritizing.

DSCP value	DSCP name	Traffic class for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (default setting)	Traffic class for MACH 4000 and PowerMICE (default setting)
0	Best Effort /CS0	1	2
1-7		1	2
8	CS1	0	0
9,11,13,15		0	0
10,12,14	AF11,AF12,AF13	0	0
16	CS2	0	1
17,19,21,23		0	1
18,20,22	AF21,AF22,AF23	0	1
24	CS3	1	3
25,27,29,31		1	3
26,28,30	AF31,AF32,AF33	1	3
32	CS4	2	4
33,35,37,39		2	4
34,36,38	AF41,AF42,AF43	2	4
40	CS5	2	5
41,42,43,44,45,47		2	5
46	EF	2	5
48	CS6	3	6
49-55		3	6
56	CS7	3	7
57-63		3	7

Table 51: Mapping the DSCP values onto the traffic classes

6 Redundancy

Under Redundancy you will find the dialogs and views for configuring and monitoring the redundancy functions:

- Link Aggregation
- Ring Redundancy
- Sub-Ring
- Ring/Network coupling
- Spanning Tree

6.1 Link Aggregation

With this dialog you can:
- display an overview of all the existing link aggregations,
- create link aggregations,
- configure link aggregations,
- allow static link aggregations, and
- Delete link aggregations.

The LACP (Link Aggregation Control Protocol based on IEEE 802.3ad) is a network protocol for dynamically bundling physical network connections. The added bandwidth of all connection lines is available for data transmission. In the case of a connection breaking down, the remaining connections take over the entire data transmission (redundancy). The load distribution between the connection lines is performed automatically.
There is link aggregation when there are at least 2 parallel redundant connection lines (known as a trunk) between 2 devices, and these lines are combined into 1 logical connection. You can use link aggregation to combine up to 8 (optimally up to 4) connection lines between devices into a trunk. Any combination of twisted pair and F/O cables can be used as the connection lines of a trunk. You configure all the connections so that the transmission speed and the duplex settings of the related ports are matching.
The maximum that can exit a device are
– 2 trunks for rail devices with 4 ports,
– 4 trunks for rail and MICE devices with 8-10 ports,
– 7 trunks for all other devices.

Note: Exclude the combination of a link aggregation with the following redundancy procedures:
- Network/Ring coupling
- MRP-Ring
- Fast HIPER-Ring
- Sub-Ring

Note: A link aggregation connects exactly 2 devices.
You configure the link aggregation on each of the 2 devices involved. During the configuration phase, you connect only one single connection line between the devices. This is to avoid loops.

Parameter	Meaning
allow static link aggregations, and	When you connect devices using multiple lines, the Link Aggregation Control Protocol (LACP) automatically prevents loops from forming. Select `Allow static link aggregation` if the partner device does not support LACP (e.g. MACH 3000).
Index	This column shows you the index under which the device uses a link aggregation as a virtual port.
Name	Here you can assign a name of your choice to this link.
Enabled	This column allows you to enable/disable a link aggregation that has been set up.
Link Trap	When you select “Link Trap”, the device generates an alarm if all the connections of the link aggregation are interrupted.
STP Mode	In the “STP Mode” column, select `on` if you have integrated the link aggregation into a Spanning Tree, or `off` if you have not.
Type	`- manual` The partner device does not support LACP, and you have selected “Allow static link aggregation”. `- dynamic` Both devices support LACP and you have not selected “Allow static link aggregation”. **Note:** If there are multiple connections between devices that all support LACP, dynamic is displayed even if “Allow static link aggregation” was selected. In this case, the devices automatically switch to “dynamic”.
Device Ports	This column displays all the ports available for the link aggregation. You can use the index to assign a link aggregation already created to each port.

Table 52: Link Aggregation

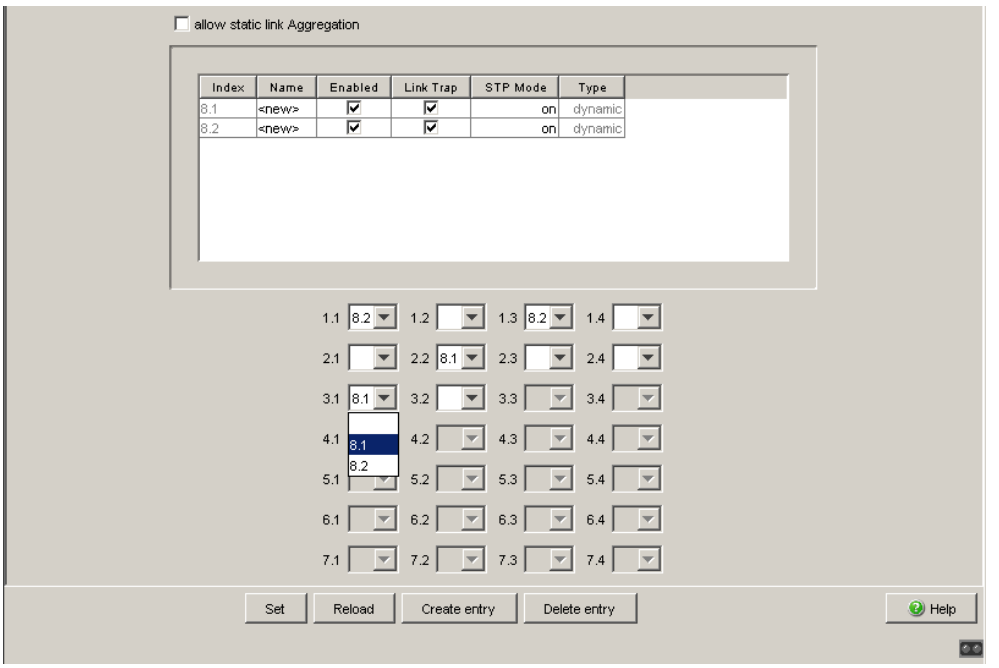


Figure 40: Setting the link aggregation

Note: For PowerMICE and MACH 4000
To increase the availability of particularly important connections, you can combine HIPER-Ring (see on page 139 “Ring Redundancy“) and link aggregation.
If you want to use a link aggregation in a HIPER-Ring, you first configure the link aggregation, then the HIPER-Ring. In the HIPER-Ring dialog, you enter the index of the desired link aggregation as the value for the module and the port (8.x). Ascertain that the respective Ring port belongs to the selected link aggregation.

6.2 Ring Redundancy

The concept of the Ring Redundancy enables the construction of high-availability, ring-shaped network structures.

If a section is down, the ring structure of a

- HIPER-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Ring with up to 50 devices typically transforms back to a line structure within 80 ms (possible settings: standard/accelerated).
- MRP (**M**edia **R**edundancy **P**rotocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).
- Fast HIPER-Ring of up to 5 devices typically transforms back to a line structure within 5 ms (maximum 10 ms). With a larger number of devices, the reconfiguration time increases.

With the help of the **R**ing **M**anager (RM) function of a device, you can connect both ends of a backbone in a line structure to form a redundant ring.

- Within a HIPER-Ring, you can use any combination of the following devices:
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100
  - MACH 1000
  - MACH 3000
  - MACH 4000
- Within an MRP-Ring, you can use devices that support the MRP protocol based on IEC62439.
- Within a Fast HIPER-Ring, you can use any combination of the following devices:
  - RSR20, RSR30
  - MACH 1000

Depending on the device model, the Ring Redundancy dialog allows you to:

- Select one of the available Ring Redundancy versions, or change it.
- Display an overview of the current Ring Redundancy configuration.
- Create new Ring Redundancies.
- Configure existing Ring Redundancies.
- Enable/disable the Ring Manager function.
- Receive Ring information.
- Delete the Ring Redundancy.

Note: Enabled Ring Redundancy methods on a device are mutually exclusive at any one time. When changing to another Ring Redundancy method, deactivate the function for the time being.

Parameter	Meaning

Version	Select the Ring Redundancy version you want to use:
	`HIPER-Ring`
	`MRP`
	`FAST HIPER-Ring` (RSR20/30, MACH 1000)
	Default setting is HIPER-Ring

Ring port No.	In a ring, every device has 2 neighbors. Define 2 ports as ring ports to which the neighboring devices are connected.
Module	Module identifier of the ports used as ring ports
Port	Port identifier of the ports used as ring ports
Operation	Value depends on the Ring Redundancy version used. Described in the following sections for the corresponding Ring Redundancy version.

Table 53: Ring Redundancy basic configuration

6.2.1 Configuring the HIPER-Ring

For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

Table 54: Port Settings for Ring Ports

Note: Configure all the devices of the HIPER-Ring individually. Before you connect the redundant line, you must complete the configuration of all the devices of the HIPER-Ring. You thus avoid loops during the configuration phase.

Note: As an alternative to using software to configure the HIPER-Ring, with the RS20/30/40, MS20/30 and PowerMICE Switches, you can also use DIP switches to enter a number of settings on the devices. You can also use a DIP switch to enter a setting for whether the configuration via DIP switch or the configuration via software has priority. The state on delivery is “Software Configuration”. You will find details on the DIP switches in the “Installation” user manual.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `active`: This port is switched on and has a link. `inactive`: This port is switched off or it has no link.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.

Table 55: HIPER-Ring configuration

Parameter	Meaning
Ring Recovery	If you are using one or multiple lines with 1,000 MBit/s twisted pair ports in the ring manager, you have the option of accelerating the reconfiguration time for when connections are interrupted. In the ring manager, select the desired value for the test packet timeout for which the ring manager waits after sending a test packet before it evaluates the test packet as lost. ▶ `Standard`: test packet timeout 480 ms ▶ `Accelerated`: test packet timeout 280 ms **Note:** Settings in the “Ring Recovery” frame are only effective for devices that are ring managers, and they are only meaningful if at least one line in the ring consists of a 1,000 MBit/s twisted pair line.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 55: HIPER-Ring configuration

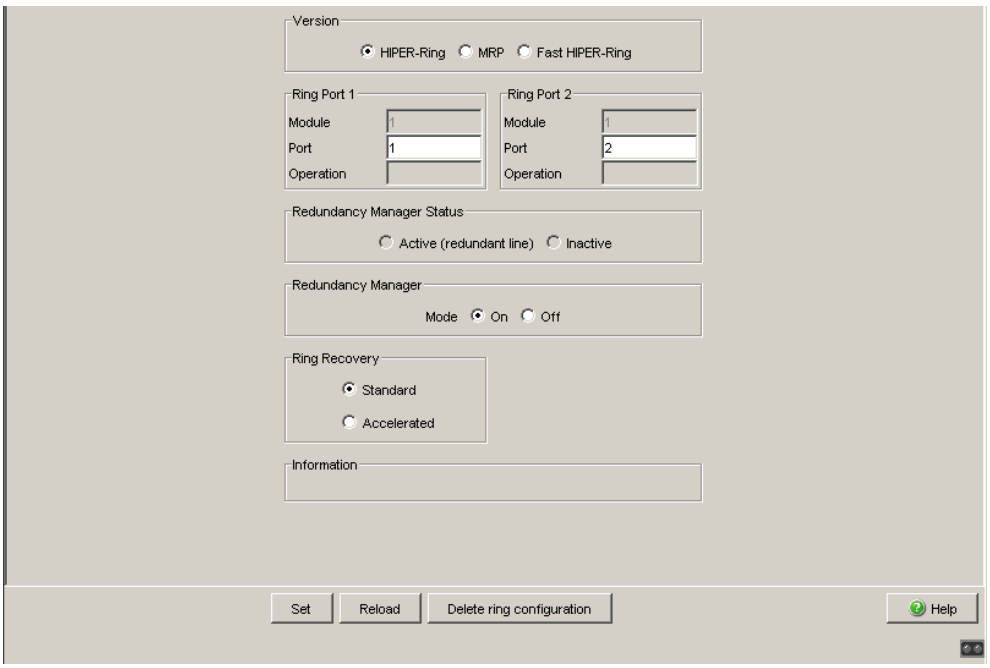


Figure 41: Selecting HIPER-Ring version, entering ring ports, enabling/disabling ring manager and selecting ring recovery (RSR20, RSR30, MACH 1000)

Note: Deactivate the Spanning Tree protocol (STP) for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (`Redundancy:Spanning Tree:Port`). If you used the DIP switch to activate the HIPER-Ring function, STP is automatically switched off.

Note: If you have configured VLANs, note the VLAN configuration of the ring ports.
In the configuration of the HIPER-Ring, you select for the ring ports
– VLAN ID 1 and
– VLAN membership Untagged in the static VLAN table

Note: If you want to use link aggregation connections in the HIPER-Ring (PowerMICE and MACH 4000), you enter the index of the desired link aggregation entry for the module and the port.

Note: When activating the HIPER-Ring function, the device sets the corresponding settings for the pre-defined ring ports in the configuration table (transmission rate and mode). If the HIPER-Ring function is switched off, the ports, which are changed back into normal ports, keep the ring port settings. Independently of the DIP switch setting, you can still change the port settings via the software.

6.2.2 Configuring the MRP-Ring

To configure an MRP-Ring, you set up the network to meet your demands. For the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Port Type	Bit Rate	Autonegotiation (Automatic Configuration)	Port Setting	Duplex Mode
Optical	all	off	on	full
TX	100 Mbit/s	off	on	full
TX	1000 Mbit/s	on	on	-

Table 56: Port Settings for Ring Ports

Note: Configure all the devices of the MRP-Ring individually. Before you connect the redundant line, you must have completed the configuration of all the devices of the MRP-Ring. You thus avoid loops during the configuration phase.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `forwarding`: This port is switched on and has a link. `blocked`: This port is blocked and has a link. `disabled`: This port is switched off. `not connected`: This port has no link.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the MRP-Ring, you switch the operation on with this setting. When you have configured all the devices in the MRP-Ring, you close the redundant line.
Ring Recovery	For the device for which you have activated the ring manager, select the value 200 ms if the stability of the ring meets the requirements of your network. Otherwise select 500 ms. `Note`: Settings in the “Ring Recovery” frame are only effective for devices that are ring managers.

Table 57: MRP-Ring configuration

Parameter	Meaning
VLAN ID	If you have configured VLANs, you select `VLAN ID 0` here if you do not want to assign the MRP-Ring configuration to a VLAN. Note the VLAN configuration of the ring ports: Select for VLAN ID 1 and VLAN membership `U` in the static VLAN table for the ring ports. `VLAN ID > 0` if you want to assign the MRP-Ring configuration to this VLAN. Select this VLAN ID in the MRP-Ring configuration for all devices in this MRP-Ring. Note the VLAN configuration of the ring ports: For all ring ports in this MRP-Ring, select this corresponding VLAN ID and the VLAN membership `T` in the static VLAN table.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 57: MRP-Ring configuration

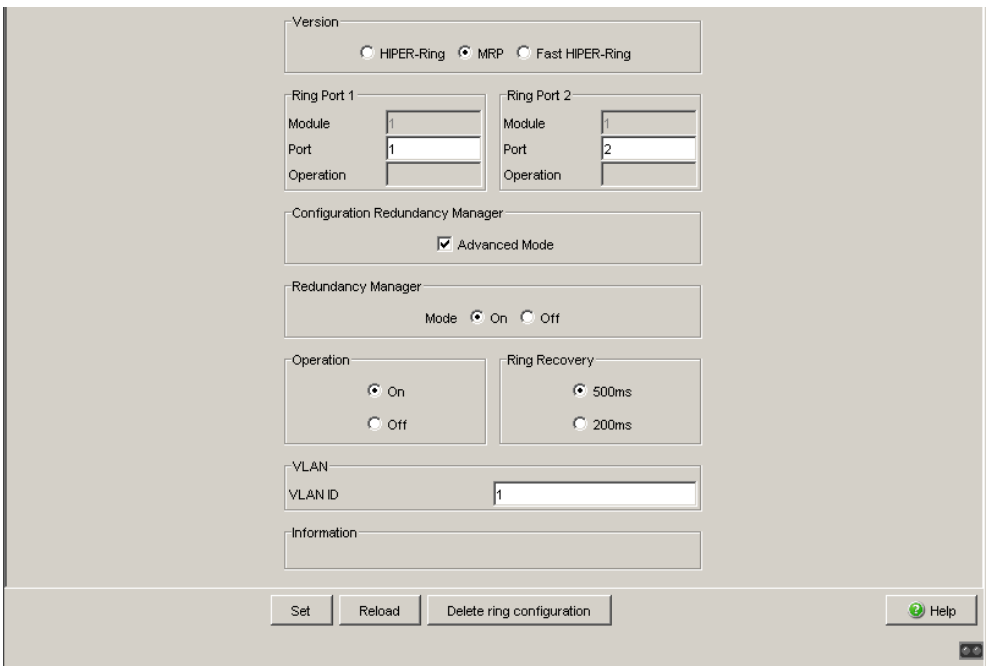


Figure 42: Selecting MRP-Ring version, entering ring ports and enabling/disabling ring manager (RSR20, RSR30, MACH 1000)

Note: For all devices in an MRP-Ring, activate the MRP compatibility in the `Redundancy:Spanning Tree:Global` dialog if you want to use RSTP in the MRP-Ring. If this is not possible, perhaps because individual devices do not support the MRP compatibility, you deactivate the Spanning Tree protocol at the ports connected to the MRP-Ring. Spanning Tree and Ring Redundancy affect each other.

Note: If you combine RSTP with an MRP-Ring, set the bridges in the MRP-Ring to a better (numerically lower) RSTP bridge priority than those in the connected RSTP network. Thus you avoid a connection interruption if connections in the MRP-Ring become inoperable.

6.2.3 Configuring the Fast HIPER-Ring (RSR20, RSR30, MACH 1000)

Within a Fast HIPER-Ring, you can use any combination of the following devices:

- RSR20, RSR30
- MACH 1000

To configure a Fast HIPER-Ring, you set up the network to meet your demands for the ring ports, select the following basic settings in the `Basic Settings:Port Configuration` dialog:

Bit rate	100 Mbit/s	1000 Mbit/s
Autonegotiation (automatic configuration)	off	on
Port	on	on
Duplex	Full	–

Table 58: Port settings for ring ports

Note: Configure all the devices of the Fast HIPER-Ring individually. Before you connect the redundant line, you must have completed the configuration of all the devices of the Fast HIPER-Ring. You thus avoid loops during the configuration phase.

Parameter	Meaning
Ring port X.X operation	Display in “Operation” field: `forwarding`: This port is switched on and has a link. `blocked`: This port is blocked and has a link. `disabled`: This port is switched off. `not connected`: This port has no link.
Redundancy Manager Mode (Ring Manager)	If there is exactly one device, you switch the Ring Manager function on at the ends of the line.
Operation	When you have configured all the parameters for the Fast HIPER-Ring, you switch the operation on here. When you have configured all the devices in the Fast HIPER-Ring, you close redundant lines.

Table 59: Fast HIPER-Ring configuration

Parameter	Meaning
Ring Information Round Trip Delay	`Round Trip Delay`: round-trip delay in µs for test packets, measured by ring manager. The display begins with 100 µs, in steps of 100 µs. Values of 1000 µs and greater indicate that the ring may become unstable. In this case, check that the number of devices in the “Switches” frame is correct (see below).
VLAN ID	If you have configured VLANs, you select `VLAN ID 0` here if you do not want to assign the Fast HIPER-Ring configuration to a VLAN. Note the VLAN configuration of the ring ports: Select for VLAN ID 1 and VLAN membership `U` in the static VLAN table for the ring ports. `VLAN ID > 0` if you want to assign the Fast HIPER-Ring configuration to this VLAN. Select the same VLAN ID in the Fast HIPER-Ring configuration for all devices in this ring. Note the VLAN configuration of the ring ports: For all ring ports in this Fast HIPER-Ring, select this corresponding VLAN ID and the VLAN membership `T` in the static VLAN table.
Switches / Number	Enter the number of devices integrated in this Fast HIPER-Ring. This entry is used to optimize the reconfiguration time and the stability of the ring.
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.

Table 59: Fast HIPER-Ring configuration

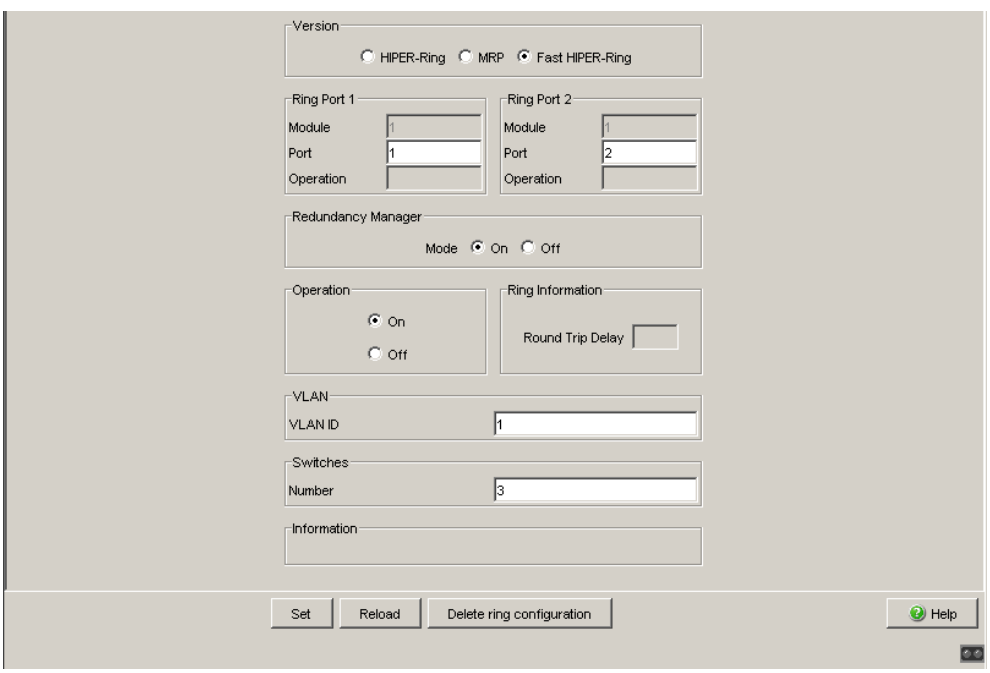


Figure 43: Selecting and configuring Fast HIPER-Ring

Note: Deactivate the Spanning Tree protocol (STP) for the ports connected to the redundant ring, because the Spanning Tree and the Ring Redundancy work with different reaction times (`Redundancy:Spanning Tree:Port`).

6.3 Sub-Ring

With this dialog you can:
- display an overview of all the connected Sub-Rings,
- create Sub-Rings,
- configure Sub-Rings, and
- Delete Sub-Rings.

Note: The following devices support the Sub-Ring Manager function:
– RSR20/RSR30
– PowerMICE
– MACH 1000
– MACH 4000

In a Sub-Ring, you can integrate as participants the devices that support MRP - the Sub-Ring Manager function is not required.

Note: Configure all the devices in the Sub-Ring before you close redundant line. You thus avoid loops during the configuration phase.

Note: Sub-Rings use MRP. You can couple Sub-Rings to existing primary rings with the HIPER-Ring protocol, the Fast HIPER-Ring protocol and MRP. If you couple a Sub-Ring to a primary ring under MRP, configure both rings in different VLANs. You configure
- either the Sub-Ring Managers' Sub-Ring ports and the devices of the Sub-Ring in a separate VLAN. Here multiple Sub-Rings can use the same VLAN.
- or the devices of the primary ring including the Sub-Ring Managers' primary ring ports in a separate VLAN. This reduces the configuration effort when coupling multiple Sub-Rings to a primary ring.

Note: In the Sub-Ring, you configure the devices with the Sub-Ring Manager functions switched off as participants of an MRP-Ring (see on page 145 “Configuring the MRP-Ring“).
This means:

- Define different VLAN membership for the primary ring and the Sub-Ring even if the primary ring uses the MRP protocol; e.g., VLAN ID 1 for the primary ring and VLAN ID 2 for the Sub-Ring.
- Switch the MRP-Ring function on for all devices.
- Switch the Ring Manager function off for all devices.
- Do not configure link aggregation.
- Switch RSTP off for the MRP-Ring ports used in the Sub-Ring.
- Assign the same MRP domain ID to all devices. If you are only using Hirschmann Automation and Control GmbH devices, you do not have to change the default value for the MRP domain ID.

Note: Use the Command Line Interface (CLI) to assign devices without the Sub-Ring Manager function a different MRP domain name. For further information, see the Command Line Interface reference manual.

6.3.1 Sub-Ring configuration

Parameter	Meaning	Possible Values	Default Setting
Max. Table Entries	Number of Sub-Rings that can be managed by a Sub-Ring Manager at the same time.		
Sub Ring ID	Unique name for this Sub-Ring.		
Function on/off	Activate the Sub-Ring only when the configuration has been completed, then close the Sub-Ring.	on off	off
Configuration State	A symbol displays the current state of the Sub-Ring.		

Table 60: Sub-Ring basic configuration

Parameter	Meaning	Possible Values	Default Setting
Redundancy exists	A symbol displays whether the redundancy exists.		
Module.Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the base ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	Target state: Define whether this SRM is to manage the redundant connection (`Redundant Manager` mode) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address will become the redundant manager. SingleManager describes the special state when a Sub-Ring is connected via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
SRM State	Current state: Shows whether this SRM manages the redundant connection (`Redundant Manager` mode) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address will become the redundant manager. `SingleManager` describes the special state when a Sub-Ring is connected via 2 ports of a single device. In this case, the port with the higher port number will manage the redundant connection.	Manager RedundantManager SingleManager	Manager
Port Status	Connection status of the Sub-Ring port	forwarding disabled blocked not connected	
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, it is created. If no separate VLAN is to be used for this Sub-Ring, leave the entry as 0.	Corresponds to the entries in the VLAN dialog	0

Table 60: Sub-Ring basic configuration

Parameter	Meaning	Possible Values	Default Setting
Partner MAC	Shows the MAC address of the Sub-Ring Manager at the other end of the Sub-Ring.	Valid MAC address	00 00 00 00 00 00
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Hirschmann devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255. 255.255.255. 255.255.255. 255.255.255. 255.255.255. 255
Protocol		standardMRP	standardMRP

Table 60: Sub-Ring basic configuration

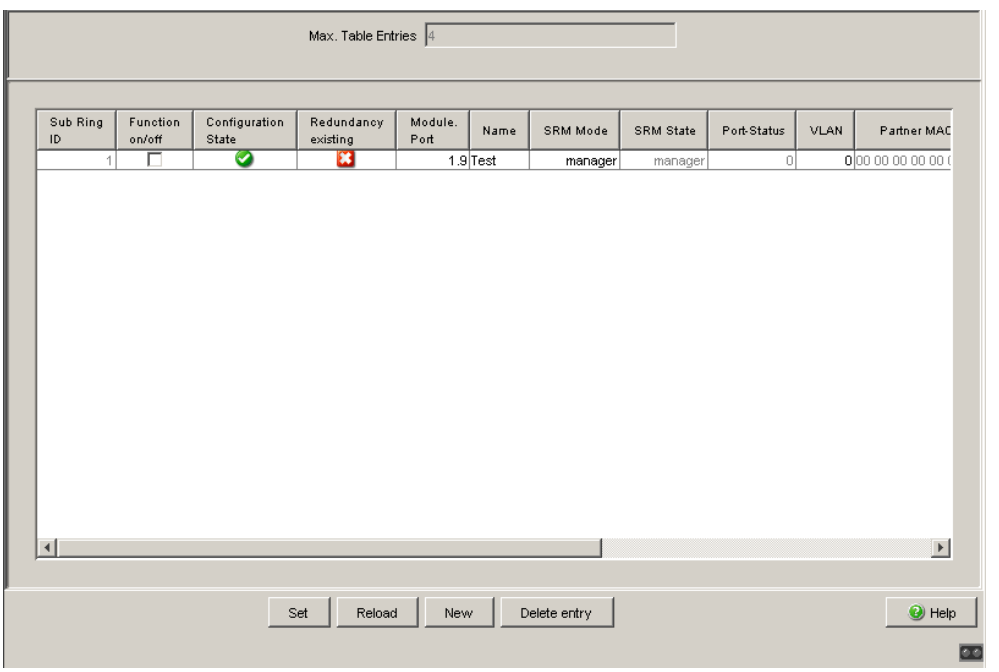


Figure 44: Sub-Ring basic configuration

6.3.2 Sub-Ring - New Entry

Parameter	Meaning	Possible Values	Default Setting
Sub Ring ID	Unique name for this Sub-Ring.		
Module.Port	ID of the port that connects the device to the Sub-Ring.	All available ports that do not already belong to the ring redundancy of the base ring, in the form X.X. (module.port)	
Name	Optional name for the Sub-Ring		
SRM Mode	Target state: Define whether this SRM is to manage the redundant connection (`Redundant Manager` mode) or not. If you have set the same value for the SRM Mode for both SRMs, the SRM with the higher MAC address will become the redundant manager. SingleManager describes the special state when a Sub-Ring is connected via 2 ports of a single device. In this case, the port with the higher port number manages the redundant connection.	Manager RedundantManager SingleManager	Manager
VLAN	VLAN to which this Sub-Ring is assigned. If no VLAN exists under the VLAN ID entered, it is created. If no separate VLAN is to be used for this Sub-Ring, leave the entry as 0.	Corresponds to the entries in the VLAN dialog	0
MRP Domain	Assign the same MRP domain name to all the members of a Sub-Ring. If you are only using Hirschmann devices, you can use the default value for the MRP domain; otherwise adjust it if necessary. With multiple Sub-Rings, all the Sub-Rings can use the same MRP domain name.	All permitted MRP domain names	255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255

Table 61: Sub-Ring - New Entry

Note: For one Sub-Ring in the `singleManager` mode, create 2 entries with different Sub-Ring IDs.

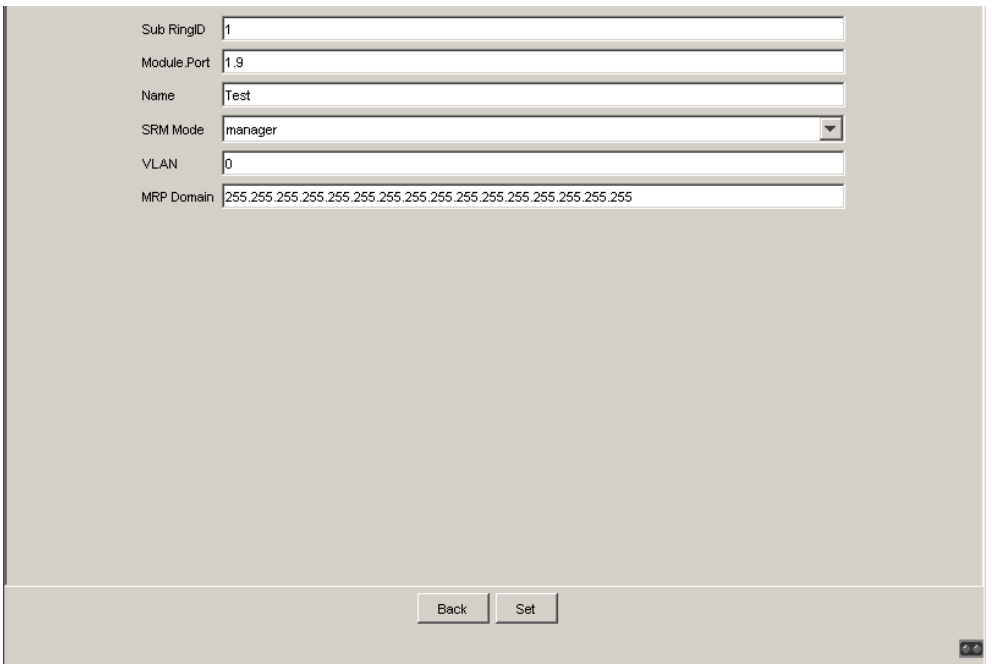


Figure 45: Sub-Ring - New Entry dialog

6.4 Ring/Network Coupling

With this dialog you can:
- display an overview of the existing Ring/Network coupling,
- configure a Ring/Network coupling,
- switch a Ring/Network coupling on/off,
- create a new Ring/Network coupling, and
- Delete Ring/Network couplings

6.4.1 Preparing a Ring/Network coupling

STAND-BY switch

All devices have a STAND-BY switch, with which you can define the role of the device within a Ring/Network coupling.
Depending on the device type, this switch is a DIP switch on the devices, or else it is exclusively a software setting (`Redundancy:Ring/Network Coupling` dialog). By setting this switch, you define whether the device has the main coupling or the redundant coupling role within a Ring/Network coupling. You will find details on the DIP switches in the “Installation” user manual.

Note: Depending on the model, the devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. When you set the DIP switches so that the software configuration is selected, the DIP switches are effectively deactivated.

Device type	STAND-BY switch type
RS2-./.	DIP switch
RS2-16M	DIP switch
RS20/RS30/RS40	Selectable: DIP switch and software setting
MICE/Power MICE	Selectable: DIP switch and software setting
MS20/MS30	Selectable: DIP switch and software setting
OCTOPUS	Software switch
RSR20/RSR30	Software switch
MACH 100	Software switch
MACH 1000	Software switch
MACH 3000/MACH 4000	Software switch

Table 62: Overview of the STAND-BY switch types

Depending on the device and model, set the STAND-BY switch in accordance with the following table:

Device with	Choice of main coupling or redundant coupling
DIP switch	On “STAND-BY” DIP switch
DIP switch/software switch option	According to the option selected - on “STAND-BY” DIP switch or in the - `Redundancy:Ring/Network Coupling` dialog, by making selection in “Select configuration”. **Note:** These devices have a DIP switch, with which you can choose between the software configuration and the DIP switch configuration. You can find details on the DIP switches in the User Manual Installation.
Software switch	In the `Redundancy:Ring/Network Coupling` dialog

Table 63: Setting the STAND-BY switch

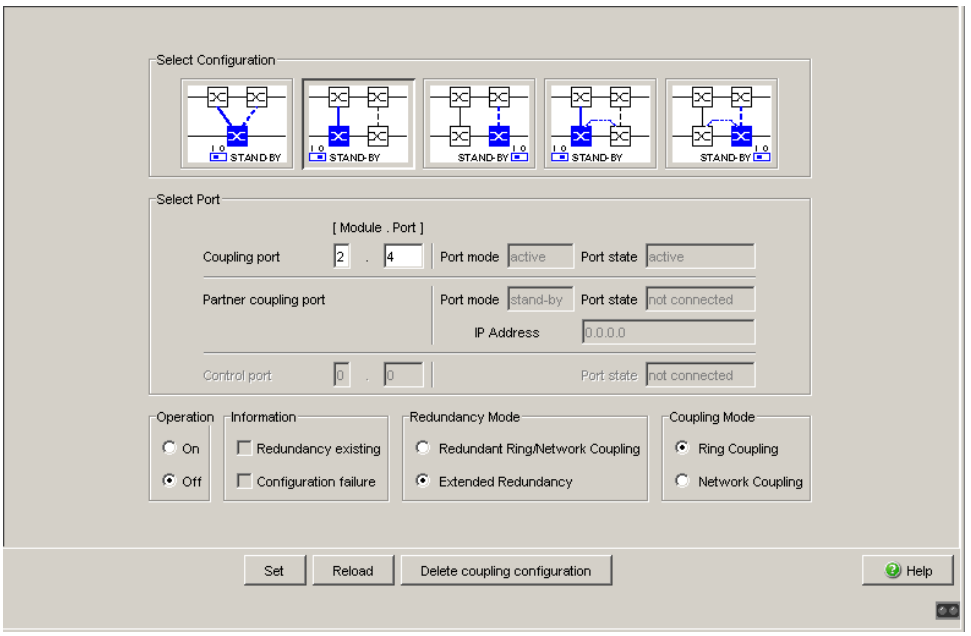


Figure 46: Software configuration of the STAND-BY switch

Depending on the STAND-BY DIP switch position, the dialog displays those configurations that are not possible as grayed-out. If you want to select one of these grayed-out configurations, change the STAND-BY DIP switch on the device to the other position.

One-Switch coupling
On the device set the 'STAND BY' dip switch to the ON position or use the software configuration to assign the redundancy function to it.

Two-Switch coupling
Assign the device in the redundant line the DIP switch setting “STAND-BY”, or use the software configuration to assign the redundancy function to it.

Note: For reasons of redundancy reliability, do not use Rapid Spanning Tree and Ring/Network Coupling in combination.

Ring/Network Coupling dialog

Parameter	Meaning
Coupling port	This is the port to which you have connected a redundant connection. **Note:** Configure the coupling port and the ring ports, if there are any ring ports, on different ports. **Note:** To avoid continuous loops, the device sets the port status of the coupling port to “off” if you switch off the function or change the configuration while the connections are operating at these ports.
Port mode	- `active` You have switched the port on. - `stand-by` The port is in stand-by mode.
Port state	- `active`: You have switched the port on. - `stand-by`: The port is in stand-by mode. - `not connected`: You have not connected the port.
Partner coupling port	This is the port at which the partner has made its connection. It is only possible or necessary to enter a port here if “One-Switch coupling” is being set up. **Note:** Configure the partner coupling port and the ring ports, if there are any ring ports, on different ports.
IP Address	If you have selected “Two-Switch coupling”, the IP address of the partner is displayed here if you have already started operating the partner in the network.
Control port	This is the port to which you connect the control line.
Operation	Here you switch the Ring/Network coupling for this device on or off
Information	If the device is a ring manager: The displays in this frame mean: “Redundancy working”: When a component of the ring is down, the redundant line takes over the function of the failed line. “Configuration failure”: You have configured the function incorrectly, or there is no ring port connection.
Redundancy Mode	With the “Redundant Ring/Network Coupling” setting, either the main line or the redundant line is active. Both lines are never active simultaneously. With the “Extended Redundancy” setting, the main line and the redundant line are simultaneously active if a problem is detected in the connection line between the devices in the connected (i.e., the remote) network. During the reconfiguration period, package duplications may possibly occur. Therefore, only select this setting if your application detects package duplications.
Coupling Mode	Here you define whether the constellation you are configuring is a coupling of redundancy rings (HIPER-Ring, MRP-Ring or Fast HIPER-Ring), or network segments.

Table 64: Ring/Network Coupling dialog

The following tables show the selection options and default settings for the ports used in the Ring/Network coupling.

Device	Partner coupling port	Coupling port
RS2-./.	Not possible	Not possible
RS2-16M	All ports (default setting: port 2)	All ports (default setting: port 1)
RS20, RS30, RS40	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
OCTOPUS	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MICE	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
PowerMICE	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MS20	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MS30	All ports (default setting: port 2.3)	All ports (default setting: port 2.4)
RSR20/30	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 100	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 1000	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)
MACH 3000	All ports	All ports
MACH 4000	All ports (default setting: port 1.3)	All ports (default setting: port 1.4)

Table 65: Port assignment for one-Switch coupling

Device	Coupling port
RS2-./.	Not possible
RS2-16M	Adjustable for all ports (default setting: port 1)
RS20, RS30, RS40	Adjustable for all ports (default setting: port 1.4)
OCTOPUS	Adjustable for all ports (default setting: port 1.4)
MICE	Adjustable for all ports (default setting: port 1.4)
PowerMICE	Adjustable for all ports (default setting: port 1.4)
MS20	Adjustable for all ports (default setting: port 1.4)
MS30	Adjustable for all ports (default setting: port 2.4)
RSR20/30	Adjustable for all ports (default setting: port 1.4)
MACH 100	Adjustable for all ports (default setting: port 1.4)
MACH 1000	Adjustable for all ports (default setting: port 1.4)
MACH 3000	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)

Table 66: Port assignment for the redundant coupling (two-Switch coupling)

Device	Coupling port	Control port
RS2-./.	Port 1	Stand-by port (can only be combined with RS2-../..)
RS2-16M	Adjustable for all ports (default setting: port 1)	Adjustable for all ports (default setting: port 2)
RS20, RS30, RS40	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
OCTOPUS	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
PowerMICE	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS20	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MS30	Adjustable for all ports (default setting: port 2.4)	Adjustable for all ports (default setting: port 2.3)
RSR20/RSR30	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 100	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 1000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)
MACH 3000	Adjustable for all ports	Adjustable for all ports
MACH 4000	Adjustable for all ports (default setting: port 1.4)	Adjustable for all ports (default setting: port 1.3)

Table 67: Port assignment for the redundant coupling (two-Switch coupling with control line)

Note: For the coupling ports, select the following settings in the `Basic Settings:Port Configuration` dialog:
– Port: on
– Automatic configuration (autonegotiation): on for twisted-pair connections
– Manual configuration: 100 Mbit/s FDX, 1 Gbit/s FDX or 10 Gbit/s FDX for glass fiber connections, depending on the port's capabilities

Note: If you have configured VLANS, note the VLAN configuration of the coupling and partner coupling ports.
In the Ring/Network Coupling configuration, select for the coupling and partner coupling ports
– VLAN ID 1 and "`Ingress Filtering`" disabled in the port table and
– VLAN membership `U` in the static VLAN table.

Note: If you are operating the Ring Manager and two-Switch coupling functions at the same time, there is the possibility of creating a loop.

6.5 Spanning Tree

Under Spanning Tree you will find the dialogs and views for configuring and monitoring the Spanning Tree function in accordance with the IEEE 802.1w (Rapid Spanning Tree, RSTP) and IEEE 802.1s (Multiple Spanning Tree, MSTP) standards.

Note: The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description employs the term bridge for Switch.

Introduction
Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus the total failure of the network. In order to avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy ensures the systematic reactivation of individual connections as needed.

Rapid Spanning Tree Protocol (RSTP)
RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge fails, the STP required a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

Note: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the Switches takes over the role of the root bridge here. The maximum number of devices permitted in a branch (from the root bridge to the tip of the branch) is specified by the variable `Max Age` for the current root bridge. The preset value for `Max Age` is 20, which can be increased up to 40. If the device working as the root fails and another device takes over its function, the `Max Age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

Note: When coupling network segments to an MRP-Ring and activating the MRP compatibility, note this special condition: If the root bridge is within the MRP-Ring, the devices within the MRP-Ring count as a single virtual device when calculating the length of the branch.

Note: The RSTP standard dictates that all the devices within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

Note: By changing the IEEE 802.1D-2004 standard for RSTP, the Standards Commission reduced the maximum value for the “Hello Time” from 10 s to 2 s. When you update the Switch software from a release before 5.0 to release 5.0 or higher, the new software release automatically reduces the locally entered “Hello Time” values that are greater than 2 s to 2 s.
If the device is not the RSTP root, “Hello Time” values greater than 2 s can remain valid, depending on the software release of the root device.

Multiple Spanning Tree Protocol (MSTP)
MSTP is a further development of the Rapid Spanning Tree Protocol used to increase the benefits of VLANs. MSTP allows you to define multiple groups of VLANs, and to configure a separate Spanning Tree Instance for each group. This Spanning Tree Instance prevents loops within the related VLAN group and provides redundancy in the case of a failure.
Additionally, MSTP enables existing connections to be used more efficiently in normal operation. For example, MSTP can set a connection between 2 bridges to the “discarding” state for a certain VLAN group, while simultaneously operating the same connection for another VLAN group in the “forwarding” state. MSTP thus enables you to use your resources more efficiently.

Note: The following text uses the term Spanning Tree (STP) to describe settings or behavior that applies to STP, RSTP or MSTP.

6.5.1 Global

With this dialog you can:
- switch the Spanning Tree Protocol on/off and select the RSTP or MSTP protocol version
- display bridge-related information on the Spanning Tree Protocol
- configure bridge-related parameters of the Spanning Tree Protocol
- set bridge-related additional functions
- display the parameters of the root bridge and
- display bridge-related topology information.

Note: Rapid Spanning Tree is activated on the device by default, and it automatically begins exploding the existing topology into a tree structure. If you have deactivated RSTP on individual devices, you avoid loops during the configuration phase.

The following tables show the selection options and default settings, and information on the global Spanning Tress settings for the bridge.

Parameter	Meaning	Possible Values	Default Setting
Frame „Function“	Switches the Spanning Tree function for this device “On” or “Off”. If you switch off the Spanning Tree for a device globally, the device floods the Spanning Tree packets received like normal Multicast packets to the ports. Thus the device behaves transparently with regard to Spanning Tree packets.	`On`, `Off`	`On`
Frame „Protocol Version“	Select the protocol version: - `RSTP (IEEE 802.1w)`, to use Spanning Tree in combination for all the configured VLANs, - `MSTP (IEEE 802.1s)`, to use Spanning Tree separately for various VLAN groups.	`RSTP (IEEE 802.1w)`, `MSTP (IEEE 802.1s)`	`RSTP (IEEE 802.1w)`

Table 68: Global Spanning Tree settings, basic function

In the “Protocol Configuration / Information” frame you can configure the following values and read information.

In the context of MSTP, these are the settings for the Common Spanning Tree (CST).

Parameter	Meaning	Possible Values	Default Setting
Column „Bridge“	**Information and configuration parameters of the local device**		
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	Sets the local bridge priority. The bridge priority and its own MAC address make up this separate `Bridge ID`. The device with the best (numerically lowest) priority becomes the root device. Define the root device by assigning the device the best (numerically lowest) priority in the `Bridge ID` among all the devices in the network. Note that you may only enter multiples of 4,096 for this value.	0 ≤ n * 4,096 ≤ 61,440	32,768
Hello Time	Sets the Hello Time. The local `Hello Time` is the time in seconds between the sending of two configuration messages (Hello packets). If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the “Root” column on the right.	1 - 2	2

Table 69: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible Values	Default Setting
Forward Delay	Sets the Forward Delay parameter. In the previous STP protocol, the Forward Delay parameter was used to delay the status change between the statuses `disabled`, `discarding`, `learning`, `forwarding`. Since the introduction of RSTP, this parameter only has a subordinate role, because the RSTP bridges negotiate the status change without any specified delay. If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the “Root” column on the right.	4 - 30 s See the note following this table.	15 s
Max Age	Sets the Max Age parameter. In the previous STP protocol, the Max Age parameter was used to specify the validity of STP BPDUs in seconds. For RSTP, Max Age signifies the maximum permissible branch length (number of devices to the root bridge). If the local device is the root, the other devices in the entire network take over this value. Otherwise the local device uses the value of the root bridge in the “Root” column on the right.	6 - 40 s See the note following this table.	20 s
TX Hold Count	Sets the HX Hold Count parameter. The TX Hold Count parameter specifies the maximum number of BPDUs that a port may send per second. If more BPDUs are waiting to be sent, the device rejects the remaining ones. When the global Hello Time has elapsed, the device sends all the currently waiting BPDUs until the maximum number is reached again.	1 - 40 (based on RSTP standard: 1 - 10)	10

Table 69: Global Spanning Tree settings, local bridge parameters

Parameter	Meaning	Possible Values	Default Setting
MRP compatibility	Switches the MRP compatibility on/off. MRP compatibility enables RSTP to be used within an MRP-Ring and when coupling RSTP segments to an MRP-Ring. The prerequisite is that all devices in the MRP-Ring must support MRP compatibility. If you combine RSTP with an MRP-Ring, set the bridges in the MRP-Ring to a better (numerically lower) RSTP bridge priority than those in the connected RSTP network. Thus you avoid a connection interruption if connections in the MRP-Ring become inoperable.	`On`, `Off`	`Off`
BPDU Guard	Switches the `BPDU Guard` function on/off. If `BPDU Guard` is switched on, the device automatically activates the function for edge ports (with the setting “Admin Edge Port” `true`). When such a port receives any STP-BPDU, the device sets the port status “BPDU Guard Effect” to `true` and the transmission status of the port to `discarding`(see table 79). Thus the device protects your network at terminal device ports from attacks with STP-BPDUs that try to change the topology.	`On`, `Off`	`Off`

Table 69: Global Spanning Tree settings, local bridge parameters

Note: The parameters `Forward Delay` and `Max Age` have the following relationship:

`Forward Delay` ≥ (`Max Age`/2) + 1

If you enter values that contradict this relationship, the device then replaces these values with the last valid values or the default value.

Parameter	Meaning	Possible Values	Default Setting
Column „Root“	**Information on the device that is currently the root bridge**		
Bridge ID	The `Bridge ID` of the current root bridge. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Priority	The `Priority` of the current root bridge.	0 ≤ n*4096 ≤ 61440	32768
Hello Time	The `Hello Time` of the current root bridge.	1 - 2	2
Forward Delay	The `Forward Delay` of the current root bridge.	4 - 30 s	30 s
Max Age	The `Max Age` of the current root bridge.	6 - 40 s	20 s

Table 70: Global Spanning Tree settings, root bridge information

Parameter	Meaning	Value range
Column „Topology“	**Spanning Tree topology information**	
Bridge is root	If the local device is currently the root bridge, the device displays this box as selected. If the device is not the root bridge, it is displayed as empty.	Selected, not selected.
Root Port	The port of the device from which the current path leads to the root bridge. 0: the local bridge is the root.	Valid port ID or 0.
Root path costs	Path costs from the root port of the device to the current root bridge of the entire layer 2 network. 0: the local bridge is the root.	0-200,000,000
Topology changes	Counts how often the device has put a port into the `Forwarding` status via Spanning Tree since it was started.	
Time since last change	Time since the last topology change.	

Table 71: Global Spanning Tree settings, topology information

If you have activated the “MRP Compatibility” function, the device displays the “Information” frame with additional information on MRP compatibility:

Parameter	Meaning	Possible Values	Default Setting
Information	If you have activated the MRP compatibility (RSTP over MRP) and one of the participating devices has detected a configuration problem, the device displays “Conflict with bridge pppp / mm mm mm mm mm”. During normal operation, this field is empty.	Message with bridge ID or empty.	-

Table 72: Global Spanning Tree settings, Information frame

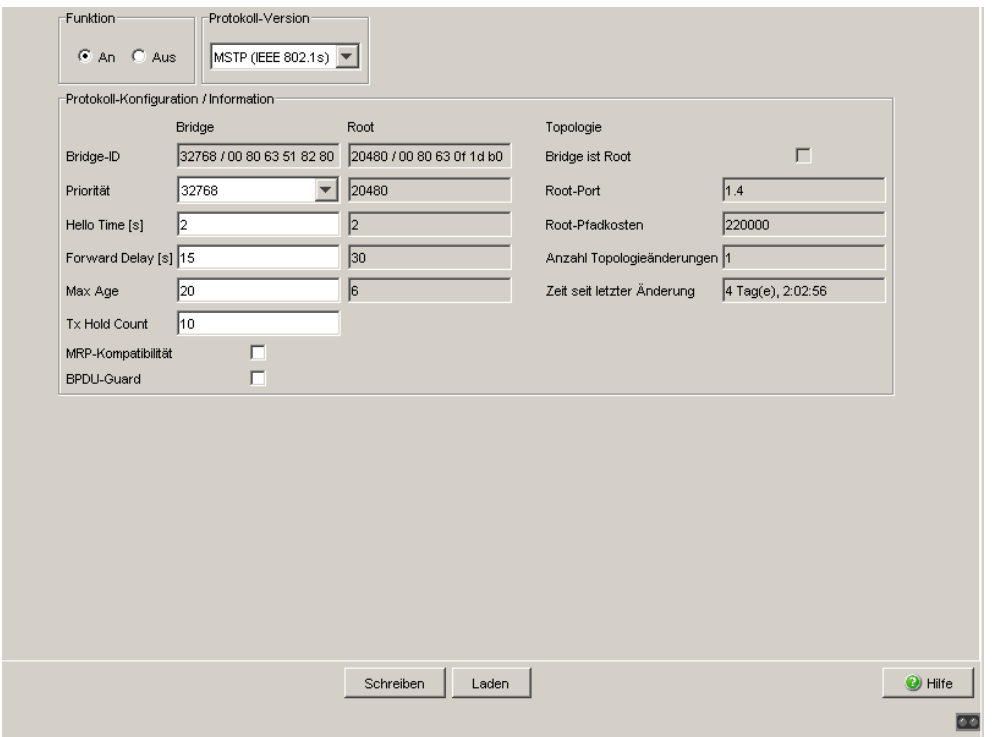


Figure 47: Dialog Spanning Tree, Global

6.5.2 MSTP (Multiple Spanning Tree)

With this dialog you can:
- manage the global Multiple Spanning Tree Instance
- create or delete a Multiple Spanning Tree Instance
- assign VLANs to a Multiple Spanning Tree Instance and manage the MSTI.

The tab for the global Multiple Spanning Tree Instance is named “MST Global (CIST)”. This instance is always available and cannot be deleted. It contains all the configured VLANs that are not explicitly assigned to an MSTI. The settings include the MST region identifier, the maximum number of Hops for the IST, and information on IST and CST (known in combination as CIST).

The tabs for the MSTIs are named MSTI, followed by the number of the instance, e.g. “MSTI 2”. Here you can manage the individual Multiple Spanning Tree Instances (MSTIs). The device allows you to create up to 16 Multiple Spanning Tree Instances (MSTIs). The prerequisite for using MSTP is that all the bridges in the network that make up an MSTP region must also support MSTP.

Note: Exclude the combination of MSTP with the following redundancy procedures and settings at the same ports:
- HIPER-Ring
- MRP-Ring
- Fast HIPER-Ring
- Sub-Ring
- Network/Ring coupling
- VLAN 0 Transparent Mode
- PROFINET IO[1]

For details of how you can configure this exclusion with maximum protocol inter-operability (see on page 179 “Port“).

1. PROFINET IO requires the VLAN 0 Transparent mode.

Note: When combining MSTP with the management VLAN 0, note the following restriction: the DHCP client of the device only sends its DHCP Broadcasts in VLAN 1.

Dialog Tab MSTP Global (CIST)

This tab in the dialog allows you to configure the MST region and the global Multiple Spanning Tree Instance (IST) within the MST region, and to display information on IST and CST.

Parameter	Meaning	Possible Values	Default Setting
Frame „MST Region Identifier“	Information on the global MST instance		
Name	Name of the MSTP region to which the device belongs.	Max. 32 characters, value 0x21 (!) up to and incl. 0x7e (~)	The MAC address of the device.
Revision level	Version number of the MSTP region to which the device belongs.	0 -65,535	0
Digest	The MD5 checksum of the MSTP configuration.	16 bytes in hexadecimal.	

Table 73: Dialog Multiple Spanning Tree settings, MST Global, MST region identifier

Note: Configure all the bridges of an MST region with identical values for:
– the MST Region Identifier,
– the Revision Level and
– the mapping of the VLANs to the MSTP instances.

Note: Include the ports that connect the bridges of an MST region as tagged members in all the VLANs that are set up on the bridges. You thus avoid potential connection breaks when the topology is changed within the MST region.
Also include the ports that connect an MST region with other MST regions or with the CST region (known as boundary ports) as tagged members in all the VLANs that are set up on both regions. You thus avoid potential connection breaks when topology changes affecting the boundary ports are made.

Parameter	Meaning	Possible Values	Default Setting
Frame „Global CIST Parameters“	Detailed information on the global MST instance (IST) for the region and CST.		
Maximum Hops	Maximum number of bridges within the MST region in a branch to the root bridge.	1 - 127	20
Assigned VLANs	List of all VLANs that are assigned only to the global MST instance and to no other MSTI.	List of all static VLANs.	1;
Bridge ID (read only)	The local Bridge ID, made up of the local priority and its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Root ID	The `Bridge ID` of the current root bridge of the entire layer 2 network.[a] The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Regional Root ID	The `Bridge ID` of the current root bridge that belongs to the global instance (IST) of the MST region to which this device belongs.[b] The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).		
Root Port	The port of the device from which the current path leads to the root bridge of the entire layer 2 network (CIST root). 0: local bridge is CIST root.	Valid port ID or 0	-

Table 74: Dialog Multiple Spanning Tree settings, MST Global (CIST), Global MST parameters

Parameter	Meaning	Possible Values	Default Setting
Root path costs	External path costs from the regional root bridge of the MST region of the device to the current root bridge of the entire layer 2 network (CIST root).[c] These are the same for all devices within an MST region. 0: Regional root bridge is simultaneously CIST root bridge	0-200,000,000	
Internal root path costs	Internal path costs from the root port of the device to the current regional root bridge of the MST region of the device. 0: local bridge is root.	0-200,000,000	-

Table 74: Dialog Multiple Spanning Tree settings, MST Global (CIST), Global MST parameters

- [a] This bridge is also known as the CIST root bridge (CIST: Common and Internal Spanning Tree). It has the best bridge ID of all bridges - both those that do not belong to any MSTP region (CST, Common Spanning Tree) and those that belong to the global instance of an MSTP region (Internal Spanning Tree, IST). All the bridges in the entire layer 2 network use the time parameters of the CIST root bridge, e.g. the Hello Time.
- [b] The IST regional root ID can be identical to the above CIST root ID for the MST region of the device if the IST regional root bridge has the best bridge ID in the entire layer 2 network.
- [c] These are identical to the root path costs from Spanning Tree or Rapid Spanning Tree if you are not using MSTP (in these cases every device sees itself as a separate region).

Parameter	Meaning	Value range
Buttons		
New	Opens a dialog for entering a new MST Instance ID. Enter the desired MSTI ID and click on the OK button. The device creates a new tab in the dialog with the name “MSTI <ID>”.	1-4094
delete it	Opens a dialog for selecting an existing MSTI ID. Select the desired MSTI ID and click on the OK button. The device deletes the tab with the name “MSTI <ID>”.	-

Table 75: Dialog Multiple Spanning Tree settings, MST Global (CIST), buttons

MSTI (Multiple Spanning Tree Instance) dialog tab

These MSTI tabs in the dialog allow you to manage the individual Multiple Spanning Tree Instances. The tab is named MSTI, followed by the number of the instance, e.g. “MSTI 2”.

Parameter	Meaning	Possible Values	Default Setting
Frame „VLANs“	Manage the VLANs assigned to this Multiple Spanning Tree Instance.		
Assigned VLANs	List of all VLANs currently assigned to this MSTI.	Subset of all statically set up VLANs.	No VLANs.
“Add VLAN” button	Opens a dialog for selecting a VLAN ID from the statically set up VLANs of the device. Select the desired VLAN ID and click on “OK”.	One of the static VLANs.	
“Remove VLAN” button	Opens a dialog for selecting a VLAN ID. Select the desired VLAN ID and click on “OK”.	A VLAN currently assigned to the MSTI	

Table 76: Multiple Spanning Tree settings, MST Instance, VLANs

Parameter	Meaning	Possible Values	Default Setting
Frame „Instance Parameters“	Detailed information on the selected Multiple Spanning Tree Instance.		
Priority	The local bridge `Priority` for the selected MST Instance. The bridge priority and its own MAC address make up this separate `Bridge ID`. The device with the best (numerically lowest) priority becomes the root device of the selected MST region. Define the root device by assigning to this device the best (numerically lowest) priority in the `Bridge ID` among all the devices in the selected MST region. Note that you may only enter multiples of 4,096 for these values.	0 ≤ n*4096 ≤ 61440	32,768
Bridge ID	The local `Bridge ID`, made up of the local `priority` + MSTI, following by its own MAC address. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority+MSTI (decimal) and mm: the respective byte of the MAC address (hexadecimal).	0 - 65,534; sum of priority (0 - 61,440 in steps of 4,096) and MSTI (1 - 4,094)	32,768 + MSTI
Time since last change	Time since the last topology change for this MST Instance.		
Topology changes	Counts how often the device has put a port into the `Forwarding` status via Spanning Tree since the selected MST Instance was started.		
Root ID	The `Bridge ID` of the current root bridge of the selected MST region. The format is ppppp / mm mm mm mm mm mm, with: ppppp: priority (decimal) and mm: the respective byte of the MAC address (hexadecimal).	0 - 65,534; sum of priority (0 - 61,440 in steps of 4,096) and MSTI (1 - 4,094)	
Root path costs	Path costs from the root port to the current root bridge of the selected MST region. 0: bridge is root for this MST region.	0-200,000,000	
Root Port	The port of the device from which the current path leads to the root bridge of the selected MST region. 0: bridge is root for this MST region.	Valid port ID or 0	

Table 77: Multiple Spanning Tree settings, MST Instance, parameters

6.5.3 Port

Note: Deactivate the Spanning Tree protocol for the ports connected to a HIPER-Ring, Fast HIPER-Ring, or Ring/Network coupling, because Spanning Tree and Ring Redundancy or Ring/Network coupling affect each other.
Activate the MRP compatibility in an MRP-Ring if you want to use RSTP and MRP in combination.
If you combine RSTP with an MRP-Ring, set the bridges in the MRP-Ring to a better (numerically lower) RSTP bridge priority than those in the connected RSTP network. Thus you avoid a connection interruption if connections in the MRP-Ring become inoperable.

These MSTI tabs in the dialog allow you to manage the individual Multiple Spanning Tree Instances. The tab is named MSTI, followed by the number of the instance, e.g. “MSTI 2”.

- switch Spanning Tree on or off at the individual ports, configure the ports for the global MST Instance (CIST), and display information on the port status,
- set various protection functions at the ports,
- configure the ports for an existing MST Instance (port path costs and port priority), read information on the port status, and display information for the selected MSTI.

Parameter	Meaning	Possible Values	Default Setting
Tab „CIST“	Port configuration and information on the global MSTI (IST) and the CST.		
STP active	Here you can switch Spanning Tree on or off for this port. If Spanning Tree is activated globally and switched off at one port, this port does not send STP-BPDUs and drops any STP-BPDUs received. **Note:** If you want to use other layer 2 redundancy protocols such as HIPER-Ring or Ring/Network coupling in parallel with Spanning Tree, make sure you switch off the ports participating in these protocols in this dialog for Spanning Tree. Otherwise the redundancy can fail or loops can result.	`On`, `Off`	`On`
Port status (read only)	Displays the STP port status with regard to the global MSTI (IST).	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-
Port role (read only)	Displays the STP port role with regard to the global MSTI (IST).	`root`, `alternate`, `designated`, `backup`, `master`, `disabled`	-
Port path costs	Enter the path costs with regard to the global MSTI (IST) to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs for the global MSTI (IST) depending on the transmission rate.	0 - 200,000,000	0 (automatically)
Port priority	Here you enter the port priority (the four highest bits of the port ID) with regard to the global MSTI (IST) as a decimal number of the highest byte of the port ID.	16 ≤ n·16 ≤ 240	128

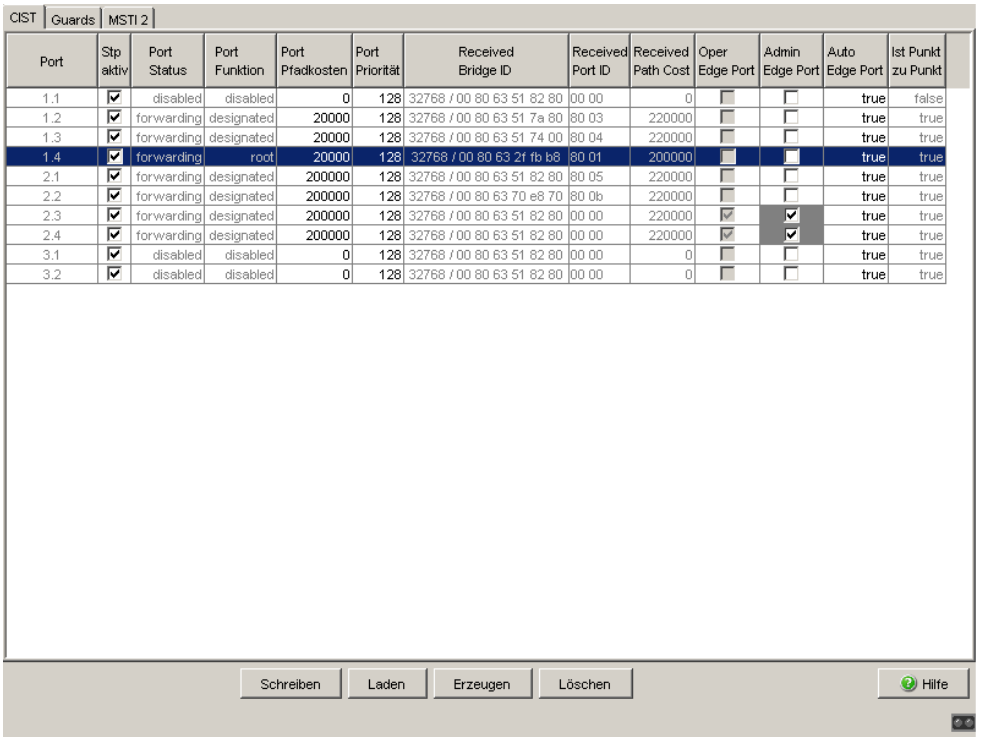
Table 78: Port-related STP settings and displays, CIST

Parameter	Meaning	Possible Values	Default Setting
Received bridge ID (read only)	Displays the remote bridge ID from which this port last received an STP-BPDU. In the stable condition (no topology change), this is usually the designated bridge ID, as only its port has the role “designated” and thus sends BPDUs.	Bridge ID (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID at the remote bridge from which this port last received an STP-BPDU. In the stable condition (no topology change), this is usually the designated port of the designated bridge, as only its port sends BPDUs.	Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)	-
Received path costs (read only)	Displays the path costs of the remote bridge from its root port to the CIST root bridge.	0-200,000,000	-
Admin Edge Port	Activate this setting when a terminal device is connected to the port. Then the port immediately has the forwarding status after a link is set up, without first going through the STP statuses. If the port still receives an STP-BPDU, the device blocks the port and clarifies its STP port role. In the process, the port can switch to a different status, e.g. `forwarding`, `discarding`, `learning`. Deactivate the setting when the port is connected to a bridge. After a link is set up, the port then goes through the STP statuses first before taking on the `forwarding` status, if applicable. This setting applies to all MSTIs.	`active` (box selected), `inactive` (box empty)	`inactive`

Table 78: Port-related STP settings and displays, CIST

Parameter	Meaning	Possible Values	Default Setting
Auto Edge Port	The Auto Edge Port setting is only considered when the Admin Edge Port parameter is deactivated. If Auto Edge Port is active, after a link is set up the device sets the port to the forwarding status after 1.5 · `Hello Time` (in the default setting 3 s). If Auto Edge Port is deactivated, the device waits for 2 · `Forward Delay` instead (in the default setting 30 s). This setting applies to all MSTIs.	`active` (box selected), `inactive` (box empty)	`active`
Oper Edge Port (read only)	The “Oper Edge Port” condition is `true` if no STP-BPDUs have been received, i.e. a terminal device is connected. It is `false` if STP-BPDUs have been received, i.e. a bridge is connected. This condition applies to all MSTIs.	`true`, `false`	-
Actual point-to-point (read only)	The “Actual point-to-point” condition is `true` if this port has a full duplex connection to an STP device, otherwise it is `false` (e.g. if a hub is connected). The point-to-point connection makes a direct connection between 2 RSTP devices. The direct, decentralized communication between the two bridges results in a short reconfiguration time. This condition applies to all MSTIs.	`true`, `false` is determined from duplex mode: FDX: `true` HDX: `false`	

Table 78: Port-related STP settings and displays, CIST



Port	Stp aktiv	Port Status	Port Funktion	Port Pfadkosten	Port Priorität	Received Bridge ID	Received Port ID	Received Path Cost	Oper Edge Port	Admin Edge Port	Auto Edge Port	Ist Punkt zu Punkt
1.1	☑	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	☐	☐	true	false
1.2	☑	forwarding	designated	20000	128	32768 / 00 80 63 51 7a 80	80 03	220000	☐	☐	true	true
1.3	☑	forwarding	designated	20000	128	32768 / 00 80 63 51 74 00	80 04	220000	☐	☐	true	true
1.4	☑	forwarding	root	20000	128	32768 / 00 80 63 2f fb b8	80 01	200000	☐	☐	true	true
2.1	☑	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	80 05	220000	☐	☐	true	true
2.2	☑	forwarding	designated	200000	128	32768 / 00 80 63 70 e8 70	80 0b	220000	☐	☐	true	true
2.3	☑	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	00 00	220000	☑	☑	true	true
2.4	☑	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	00 00	220000	☑	☑	true	true
3.1	☑	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	☐	☐	true	true
3.2	☑	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	☐	☐	true	true

Figure 48: STP Port dialog, CIST tab

Parameter	Meaning	Possible Values	Default Setting
Tab „Guards“	Protective settings for the ports.		
Root Guard	The “Root Guard” setting is only relevant for edge ports (ports with the “Admin Edge Port” setting `true`). If such a port receives an STP-BPDU with better path information on the root that what the device knows, the device discards the BPDU and sets the port status to `discarding`, instead of assigning the port the STP port role `root`. Thus the device protects your network from attacks with STP-BPDUs that try to change the topology, and from incorrect configurations. If there are no STP-BPDUs with better path information on the root, the device resets the transmission status of the port according to the port role. **Note:** The “Root Guard” and “Loop Guard” settings are mutually exclusive. If you activate one setting when the other is already active, the device switches off the other one.	`active` (box selected), `inactive` (box empty)	`inactive`
TCN Guard	If the “TCN Guard” setting is active (TCN: Topology Change Notification) the port ignores the topology change flag in the STP-BPDUs that is reporting a topology change. Thus the device protects your network from attacks with STP-BPDUs that try to change the topology, and from incorrect configurations. If the “TCN Guard” setting is inactive, the device follows the protocol in reacting to the STP-BPDUs received. **Note:** If the received BPDU contains other information apart from the topology change flag that causes a topology change (e.g. better path information on the root than that known by the device), the device processes this information.	`active` (box selected), `inactive` (box empty)	`inactive`

Table 79: Port-related STP settings and displays, guards

Parameter	Meaning	Possible Values	Default Setting
Loop Guard	The “Loop Guard” setting is only meaningful for ports with the STP role `alternate`, `backup` or `root`. If the “Loop Guard” setting is active and the port has not received any STP-BPDUs for a while, the device sets the port to the `discarding` condition (port sends no more data). The device also sets the port to what is known as the “loop status”. This is displayed in the “Loop Status” column. The device thus prevents a potential loop if no more STP-BPDUs are received if, for example, STP is switched off on the remote device, or the link only fails in the receiving direction. When the port receives BPDUs again, the device resets the loop status of the port to `false`, and the transmission status of the port according to the port role. If the “Loop Guard” setting is inactive, however, the device sets the port to the `forwarding` status when STP-BPDUs have not been received. **Note:** The “Root Guard” and “Loop Guard” settings are mutually exclusive. If you activate one setting when the other is already active, the device switches off the other one.	`active` (box selected), `inactive` (box empty)	`inactive`
Loop Status (read only)	Display the status of the Loop Status. The device sets the loop status of the port to `true` if the “Loop Guard” setting is active at the port and the port is not receiving any more STP-BPDUs. Here the device leaves the port in the `discarding` transmission status, to prevent a potential loop. When the port receives STP-BPDUs again, the device resets the loop status to `false`.	`true`, `false`	-
Transitions to Loop Status (read only)	Counts how often the device has set the port to the loop status (“Loop Status” column `true`).	0 - 4,294,967,295 (2^{32}-1)	0

Table 79: Port-related STP settings and displays, guards

Parameter	Meaning	Possible Values	Default Setting
Transitions from Loop Status	Counts how often the device has set the port out of the loop status (“Loop Status” column `true`).	0 - 4,294,967,295 (2^{32}-1)	0
BPDU Guard Effect (read only)	The “BPDU Guard Effect” status is only relevant for edge ports (ports with the “Admin Edge Port” status `true`), and only if the “BPDU Guard” global function is active (see table 69). When such a port receives any random STP-BPDU, the device sets the port's “BPDU Guard Effect” status to `true` and its transmission status to `discarding`. Thus the device protects your network at terminal device ports from attacks with STP-BPDUs that try to change the topology. To return the port to a normal transmitting status from the locked status, break and reconnect the link, or switch the “Admin Edge Port” port setting off and on again.	`true`, `false`	-

Table 79: Port-related STP settings and displays, guards

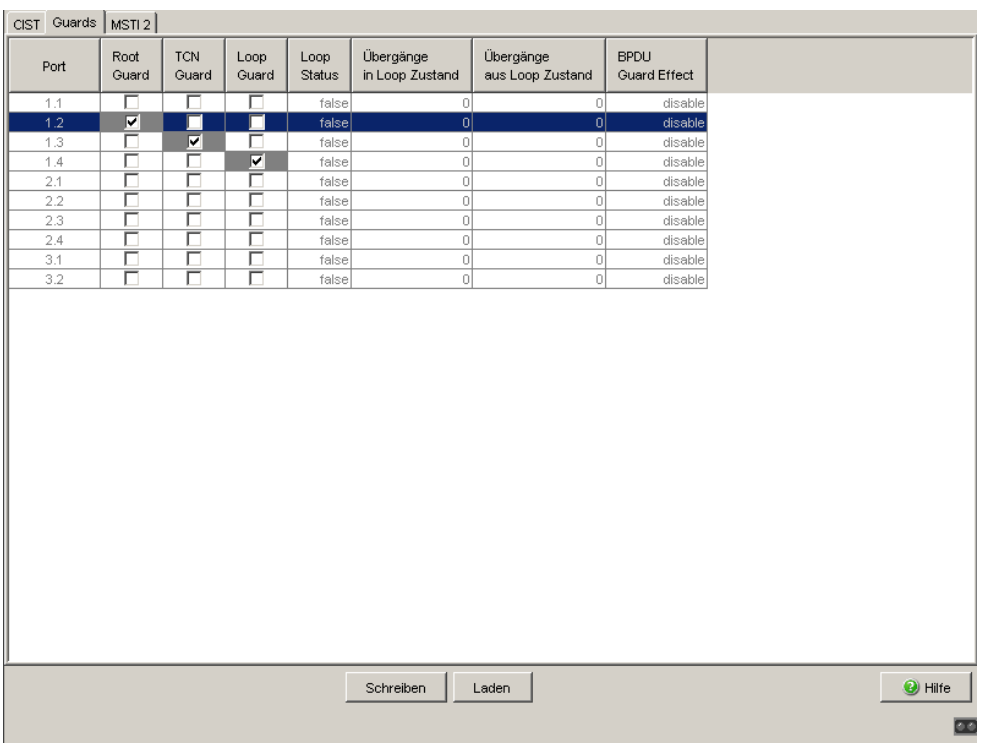


Figure 49: STP Port dialog, Guards tab

Parameter	Meaning	Possible Values	Default Setting
Tab „MSTI <ID>“	Port configuration and information on the selected MSTI.		
Port status (read only)	Displays the STP port status with regard to the current MSTI.	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-
Port role (read only)	Displays the STP port role with regard to the current MSTI.	`root, alternate, designated, backup, master, disabled`	-
Port path costs	Enter the path costs with regard to the current MSTI to indicate preference for redundant paths. If the value is 0, the Switch automatically calculates the path costs depending on the transmission rate.	0 - 200.000.000	0 (automatically)
Port priority	Here you enter the port priority (the four highest bits of the port ID) with regard to the current MSTI as a decimal number of the highest byte of the port ID.	16 ≤ n*16 ≤ 240	128
Received bridge ID (read only)	Displays the remote bridge ID of the current MSTI from which this port last received a BPDU.[a].	Bridge ID (format ppppp / mm mm mm mm mm mm)	-
Received port ID (read only)	Displays the port ID of the remote bridge of the current MSTI from which this port last received a BPDU.[a]	Port ID, format pn nn, with p: port priority / 16, nnn: port No., (both hexadecimal)	-
Received path costs (read only)	Displays the path costs of the remote bridge from its root port to the root bridge of the current MSTI.[a].	0-200,000,000	-

Table 80: Port-related STP settings and displays, per MSTI

– [a] These columns show you detailed information over and above the standard information.
For designated ports, the device displays the information for the STP-BPDU last received by the port. This helps with the diagnosis of possible STP problems in the network.

For alternative, back-up and root ports, this information is in the stationary condition (static topology), identically to that of the STP standard.
If a port has no link, or if it has not received any STP-BDPUs for the current MSTI, the device displays the values that the port would send as a designated port.

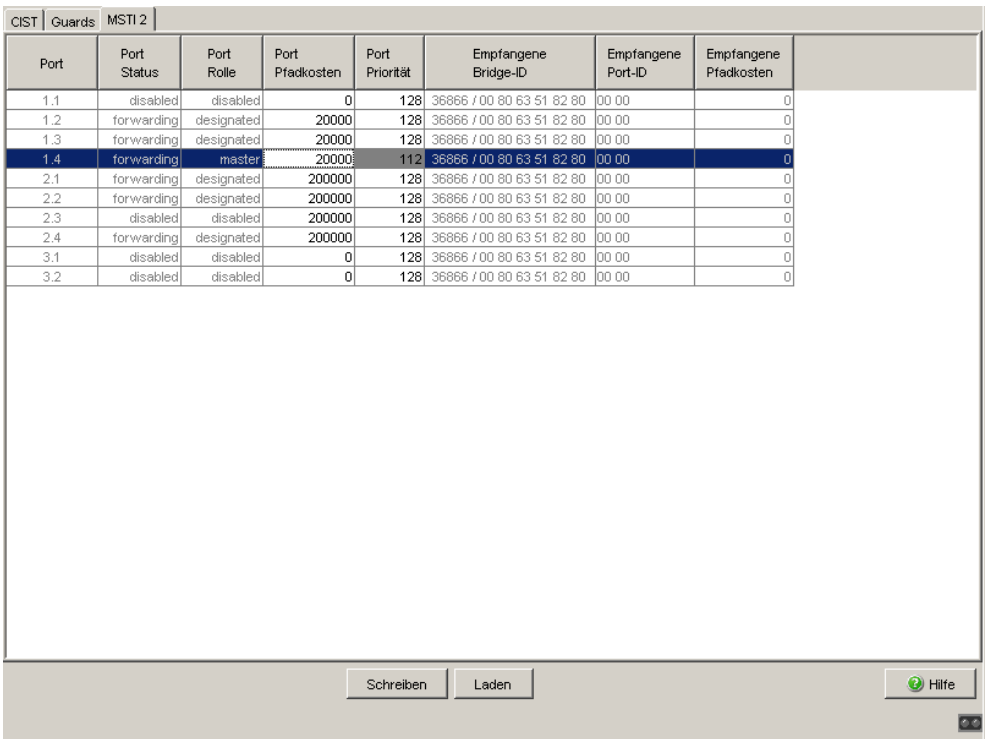

CIST
Guards
MSTI 2
Port
Port Status
Port Rolle
Port Pfadkosten
Port Priorität
Empfangene Bridge-ID
Empfangene Port-ID
Empfangene Pfadkosten
1.1 disabled disabled 0 128 36866 / 00 80 63 51 82 80 00 00 0
1.2 forwarding designated 20000 128 36866 / 00 80 63 51 82 80 00 00 0
1.3 forwarding designated 20000 128 36866 / 00 80 63 51 82 80 00 00 0
1.4 forwarding master 20000 112 36866 / 00 80 63 51 82 80 00 00 0
2.1 forwarding designated 200000 128 36866 / 00 80 63 51 82 80 00 00 0
2.2 forwarding designated 200000 128 36866 / 00 80 63 51 82 80 00 00 0
2.3 disabled disabled 200000 128 36866 / 00 80 63 51 82 80 00 00 0
2.4 forwarding designated 200000 128 36866 / 00 80 63 51 82 80 00 00 0
3.1 disabled disabled 0 128 36866 / 00 80 63 51 82 80 00 00 0
3.2 disabled disabled 0 128 36866 / 00 80 63 51 82 80 00 00 0
Schreiben
Laden
Hilfe

Figure 50: STP Port dialog, MSTI <ID> tab

7 Advanced

The menu contains the dialogs, displays and tables for:

- DHCP Relay Agent
- DHCP Server
- Industry Protocols
- Command Line

7.1 DHCP Relay Agent

This dialog allows you to configure the DHCP relay agent.

☐ Enter the DHCP server IP address.
If one DHCP server is not available, you can enter up to 3 additional DHCP server IP addresses so that the device can change to another DHCP server.

☐ With Option 82, a DHCP relay agent which receives a DHCP request adds an “Option 82” field to the request, as long as the request received does not already have such a field.
When the function is switched off, the device will forward attached “Option 82” fields, but it will not add any on. Under “Type”, you specify the format in which the device recognition of this device is entered in the “Option 82” field by the DHCP relay agent.
The options are:
– IP address
– MAC Address (state on delivery)
– System name (client ID)
– Other (freely definable ID, which you can specify in the following rows).
“Remote ID entry for DHCP server” shows you the value which you enter when configuring your DHCP server. “Type display” shows the device recognition in the selected form.

▶ The “Circuit ID” column shows you the value which you enter when configuring your DHCP server. The “Circuit ID” contains the port number and the ID of the VLAN from which the DHCP has been received.

Example of a configuration of your DHCP server:
Type: `mac`
DHCP server for RemoteID entry: `00 06 00 80 63 00 06 1E`
Circuit ID: `B3 06 00 00 01 00 01 01`
This results in the entry for the “Hardware address” in the DHCP server:
`B30600000100010100060080630006 1E`

☐ In the “Option 82 on” column, you can switch this function on/off for each port.

☐ In the “Hirschmann Device” column, you mark the ports to which a Hirschmann device is connected.

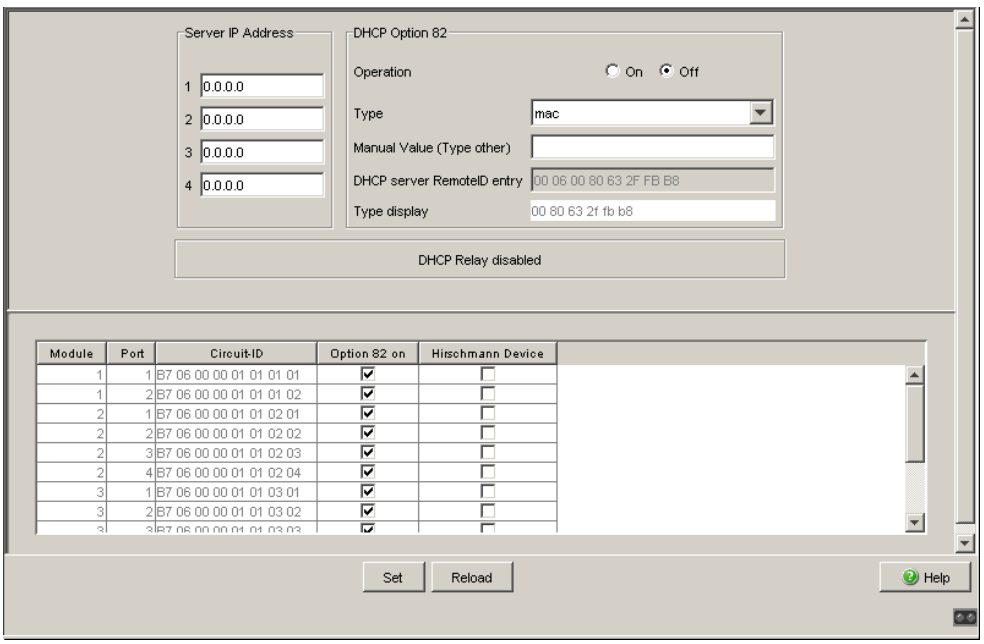

Server IP Address
1 0.0.0.0
2 0.0.0.0
3 0.0.0.0
4 0.0.0.0
DHCP Option 82
Operation
On
Off
Type
mac
Manual Value (Type other)
DHCP server RemoteID entry
00 06 00 80 63 2F FB B8
Type display
00 80 63 2f fb b8
DHCP Relay disabled
Module
Port
Circuit-ID
Option 82 on
Hirschmann Device
1 1 B7 06 00 00 01 01 01 01
1 2 B7 06 00 00 01 01 01 02
2 1 B7 06 00 00 01 01 02 01
2 2 B7 06 00 00 01 01 02 02
2 3 B7 06 00 00 01 01 02 03
2 4 B7 06 00 00 01 01 02 04
3 1 B7 06 00 00 01 01 03 01
3 2 B7 06 00 00 01 01 03 02
Set
Reload
Help

Figure 51: DHCP Relay Agent dialog

7.2 DHCP Server

The DHCP Server dialogs allow you to very easily include new devices (clients) in your network or exchange them in your network: When you select DHCP as the configuration mode for the client, the client gets the configuration data from the DHCP server.

The DHCP server assigns to the client:

– a fixed IP address (static) or an address from an address range (dynamic),
– the netmask,
– the gateway address,
– the DNS server address,
– the WINS server address and
– the lease time.

You can also specify globally or for each port a URL for transferring additional configuration parameters to the client.

7.2.1 Global

This dialog allows you to switch the DHCP server of the device on and off globally and for each port.

Parameter	Meaning	Value range	Default setting
Global settings			
DHCP server mode	Switching the DHCP server on and off globally on the device.	`On`, `Off`	`Off`
Settings per port (table)			
Port	Module and port numbers to which this entry applies.	-	-
DHCP Server active	Switch the DHCP server on and off at this port. To activate the DHCP server at a port, also switch the DHCP server mode on globally.	`On`, `Off`	`On`

Table 81: Activating/deactivating the DHCP server globally and per port

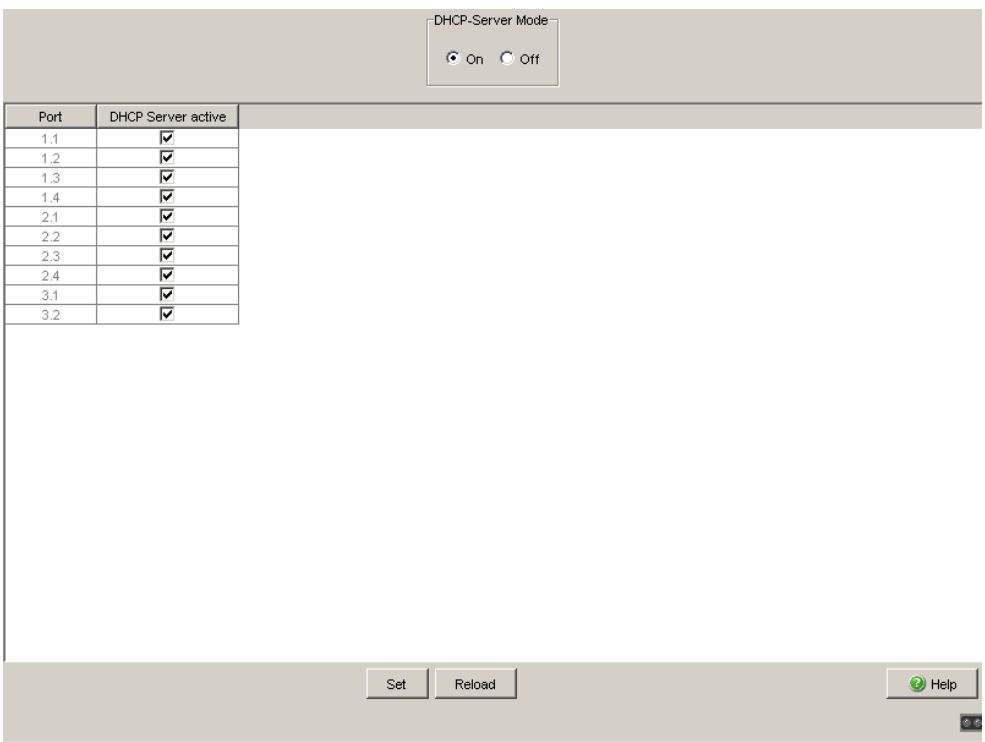


Figure 52: DHCP Server global dialog

7.2.2 Pool

This dialog allows you to closely control the allocation of IP addresses. For this purpose, the DHCP server provides what is known as an IP address pool (in short “pool”) from which it allocates IP addresses to clients. The pool consists of a list of entries. An entry can define a specific IP address or a connected IP address range.
You can choose between dynamic and static allocation.

- An entry for dynamic allocation applies to all the ports of the device for which you activate the DHCP server. If a client makes contact at a port, the DHCP server allocates a free IP address from a pool entry for this port. For dynamic allocation, create a pool entry for all ports and enter the first and last IP addresses for the IP address range. Leave the MAC Address, Client ID, Remote ID and Circuit ID fields empty.
  You have the option to create multiple pool entries. You can thus create IP address ranges that contain gaps.
- With static allocation, the DHCP server always allocates the same IP address to a client. The DHCP server identifies the client using a unique hardware ID.
  A static address entry can only contain 1 IP address, and it can apply for all ports or for a specific port of the device.
  For static allocation, create a pool entry for all ports or one specific port, enter the IP address, and leave the “Last IP Address” field empty. Enter a hardware ID with which the DHCP server uniquely identifies the client. This ID can be a MAC address, a client ID, a remote ID or a circuit ID. If a client makes contact with a known hardware ID, the DHCP server allocates the static IP address.

The table shows you the configured entries of the DHCP server pool. You have the option to create a new entry, edit an existing entry or delete entries. You have the option to create up to 64 pool entries (128 for the PowerMICE and MACH devices).

Click “Create entry” to create a new entry. The device displays a new dialog. Fill in the fields you require, then click “Write”. Click on “Back” to return to the “DHCP Server Pool” dialog.

Parameter	Meaning	Value range	Default setting
Port	Module and port numbers to which this entry applies. ▶ For a dynamic address entry select `all`. ▶ For a static address entry select all or one valid module and port number.	Valid module and port number or `all`.	`all`
Active	Activates or deactivates the pool entry.	`On`, `Off`	`Off`
IP address	▶ For a dynamic address entry: the 1st address of the IP address pool that the DHCP server is to allocate to a client. ▶ For a static address entry: the IP address that the server is always to allocate to the same client.	Valid IPv4 address	-
Last IP Address	For a dynamic address entry: the last address of the IP address pool that the DHCP server is to allocate to a client.	Valid IPv4 address	-

Table 82: DHCP server pool settings, IP address basic settings

Parameter	Meaning	Value range	Default setting
Lease time [s]	Time in s for which the DHCP server allocates the address to the client. Within the lease time, the client can apply for an extension. If the client does not apply for an extension, after it has elapsed the DHCP server takes the IP address back into the pool and allocates it to any client that requires it.	1 s - 4,294,967,295 s (2^{32}-1 s)	86,400 s (1 day)
MAC Address	For a static address entry: MAC address with which the client identifies itself.	MAC address of the client that contains the static IP address	-
Gateway	IP address of the DHCP relay via which the client makes its request. If the DHCP server receives a request via another DHCP relay, it ignores this. If there is no DHCP relay between the client and the DHCP server, leave these fields empty.	IPv4 address of the DHCP relay.	-
Client ID	For a static address entry: Client ID with which the client identifies itself.	Client ID of the client that contains the static IP address[a]	-
Remote ID	For a static address entry: Remote ID with which the client identifies itself.	Remote ID of the client that contains the static IP address[a]	-
Circuit ID	For a static address entry: Circuit ID with which the client identifies itself.	Circuit ID of the client that contains the static IP address[a]	-
Hirschmann Device	Activate this setting if the device from this entry only serves devices from Hirschmann.	`On`, `Off`	`Off`

Table 83: DHCP server pool settings, mode of address allocation

– [a] A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

Parameter	Meaning	Value range	Default setting
Configuration URL	TFTP URL, from which the client can obtain additional configuration information. Enter the URL in the form tftp://server name or ip address/ directory/file.	Valid TFTP URL	-
Default Gateway	Default gateway entry for the client.	Valid IPv4 address	-
Netmask	Netmask entry for the client.	Valid IPv4 netmask	-
WINS Server	WINS (Windows Internet Name Service) entry for the client.	Valid IPv4 address	-
DNS Server	DNS server entry for the client.	Valid IPv4 address	-
Host name	Host name for the client. If this name is entered, it overwrites the system name of the client (see on page 17 “System Data“).	Max. 64 ASCII characters in the range 0x21 (!) - 0x7e (~).	- (no host name)

Table 84: DHCP server pool settings, option allocation to the client

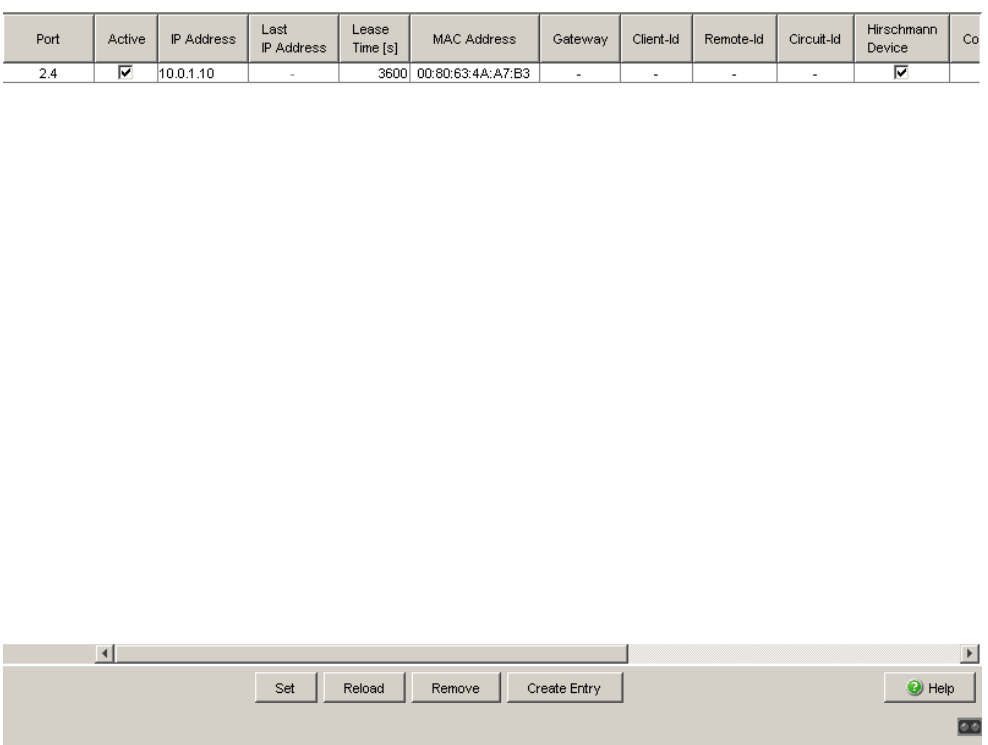


Figure 53: DHCP server pool dialog

7.2.3 Lease Table

The lease table shows you the IP addresses that the DHCP server has currently allocated.
The device displays the related details for every IP address allocated.

Parameter	Meaning	Value range
Port	Module and port numbers to which this entry applies.	-
IP address	IP address that the DHCP server has allocated to the device with the specified MAC address.	An IPv4 address from the pool.
Status	Status of the DHCP address allocation according to the Dynamic Host Configuration Protocol.	`bootp`, `offering`, `requesting`, `bound`, `renewing`, `rebinding`, `declined`, `released`
Remaining lease time [s]	Time remaining in seconds until the validity of the IP address elapses, unless the client applies for an extension.	-
Leased MAC Address	MAC address of the client that is currently leasing the IP address.	Format xx:xx:xx:xx:xx
Gateway	IP address of the DHCP relay via which the client has made the request.	IPv4 address or empty
Local (client) ID	The client ID that the client submitted for the DHCP request.	[a]
Remote ID	The remote ID that the client submitted for the DHCP request.	[a]
Circuit ID	The circuit ID that the client submitted for the DHCP request.	[a]

Table 85: DHCP lease table

– [a] A client, remote or circuit ID consists of 1 - 255 bytes in hexadecimal form (00 - ff), separated by spaces.

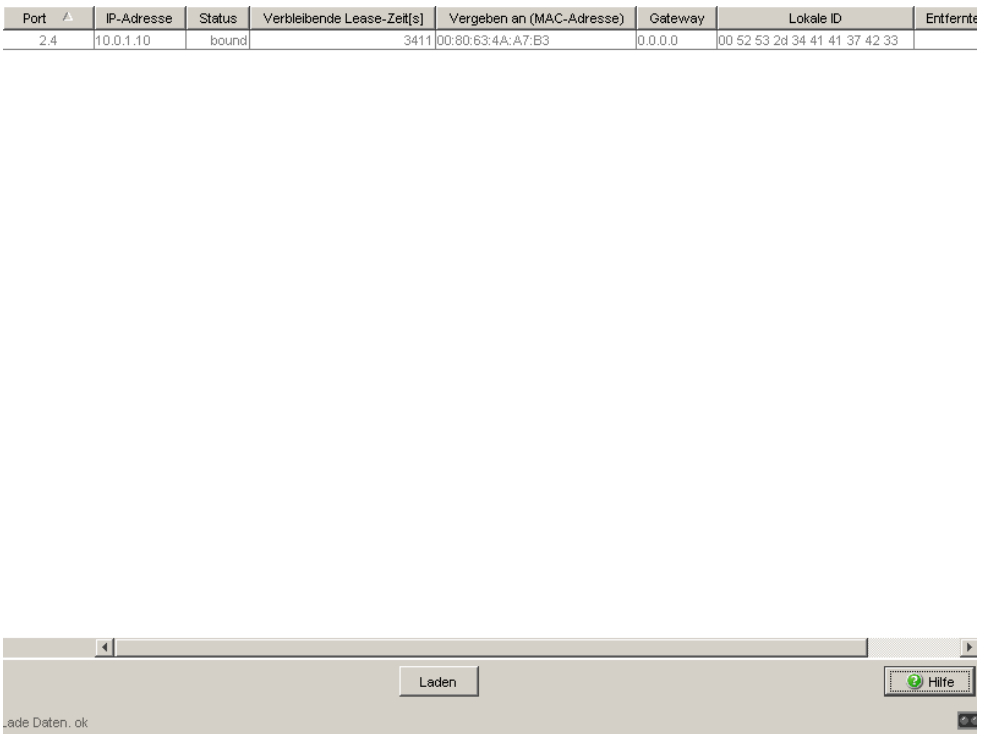


Figure 54: DHCP server lease table dialog

7.3 Industrial Protocols

The “Industry Protocols” menu allows you to
- configure the PROFINET IO protocol as well as
- the EtherNet/IP protocol.

Detailed information on industrial protocols and PLC configuration is contained in the User Manual "Industrial Protocols“.

7.3.1 PROFINET IO

This dialog allows you to configure the PROFINET IO protocol. To integrate this in a control system, perform the following steps.

General settings:

☐ In the `Basic Settings:Network` dialog, check whether `Local` is selected in the “Mode” frame (see on page 22 “Network“).

☐ In the `Switching:VLAN:Global` dialog, check whether “VLAN 0 Transparent Mode” is selected (see on page 110 “VLAN Global“).

Note: Exclude a combination of the VLAN 0 Transparent mode and the use of MSTP (Multiple Spanning Tree).

☐ Configure the alarm settings and the threshold values for the alarms you want to monitor (see on page 224 “Device Status“).

Global PROFINET IO settings:

☐ Switch on the function by selecting “ProfinetIO”.

☐ Click on “Download GSDML File” to load the GSDML file onto your PC.

PROFINET IO Port settings:

☐ Select the port for which you want to set the DCP mode in detail, and in the column `DCP Mode`, select

- `none`:
  The device sends received DCP frames. However, the CPU does not process them yet, it still generates DPC frames. The port does not send any DCP frames which were received at another port.
- `ingress`:
  The device sends received DCP frames. The CPU processes received DCP frames from this port, but does not generate any. The port does not send any DCP frames which were received at another port.
- `egress`:
  The device sends received DCP frames. The CPU ignores frames received from this port and generates them as needed.
- `both`:
  The device sends received DCP frames. The CPU processes received frames and generates them as needed.

The default setting is `both`.

Note: If you connect 2 switches which are to reside in separate DCP domains, on **both** switches you set the DCP mode of the involved ports to “none” or “ingress”. This ensures that neither of the switches receives or forwards DCP frames.

☐ Select the port for which you want to set its PHY module to the fast start mode, and select from the following in the column `Fast Start Up`:
- `disable` to set the normal start mode,
- `enable` to set the fast start mode.

Note: The setting `enable` only becomes effective if the automatic configuration of the port (Autoneg) is switched off (see on page 27 “Port Configuration“).

The default setting is `disable`. If a port does not support the fast start mode, the device will show `unsupported` in this column.

Settings for the PLC:

☐ Configure the PLC as described in the “Industry Protocols” user manual.

7.3.2 EtherNet/IP

This dialog allows you to activate the EtherNet/IP protocol. To integrate this in a control system, perform the following steps.

General settings:

☐ In the `Switching:Multicasts:IGMP` dialog, check whether IGMP Snooping is activated (see on page 100 “IGMP (Internet Group Management Protocol)“).

Global EtherNet/IP settings:

☐ Activate the function in the “EtherNet/IP” frame; the default setting is off.
☐ Click on “Download EDS File” to load the EDS file onto your PC.

Settings for the PLC:

☐ Configure the PLC as described in the “Industry Protocols” user manual.

7.4 Command Line

This window enables you to access the Command Line Interface (CLI) using the Web interface.

You will find detailed information on CLI in the “Command Line Interface” reference manual.

8 Diagnostics

The diagnosis menu contains the following tables and dialogs:

- Syslog
- Event Log
- Ports (statistics, utilization, SFP modules, TP cable diagnosis)
- Configuration Check
- Topology Discovery
- Port Mirroring
- Device Status
- Signal Contact
- Alarms (Traps)
- Report (log file, system information)
- IP Address Conflict Detection
- Self Test
- Service Mode

In service situations, they provide the technician with the necessary information for diagnosis.

8.1 Syslog

The “Syslog” dialog enables you to additionally send to one or more syslog servers, the events that the device writes to its event log. You can switch the function on or off, and you can manage a list of up to 8 syslog server entries. You also have the option to specify that the device informs various syslog servers, depending on the minimum “level to report” of the event.

Additionally, you can also send the SNMP requests to the device as events to one or more syslog servers. Here you have the option of treating GET and SET requests separately, and of assigning a “level to report” to the requests to be logged.

Note: You will find the actual events that the device has logged in the “Event Log” dialog (see on page 211 “Event Log“) and in the log file (see on page 234 “Report“), a HTML page with the title “Event Log”.

The device evaluates SNMP requests as events if you have activated “Log SNMP Set/Get Request” (see table 87).

Parameter	Meaning	Possible Values	Default Setting
Frame „Function“	Switches the syslog function for this device “On” or “Off”	`On`, `Off`	`Off`
Frame „SNMP Logging“	Settings for sending SNMP requests to the device as events to the list of syslog servers.		
Log SNMP Get Requests.	Creates events for the syslog for SNMP Get requests with the specified “level to report”.	`active`, `inactive`	`inactive`
Level to Report (for logs of SNMP Get Requests)	Specifies the level for which the device creates the event “SNMP Get Request received” for the list of the syslog servers.	`debug`, `informational`, `notice`, `warning`, `error`, `critical`, `alert`, `emergency`	`notice`

Table 86: Syslog and SNMP Logging settings

Log SNMP Set Requests.	Creates events for the syslog for SNMP Set requests with the specified “level to report”.	`active`, `inactive`	`inactive`
Level to Report (for logs of SNMP Set Requests)	Specifies the level for which the device creates the event “SNMP Set Request received” for the list of the syslog servers.	`debug`, `informational`, `notice`, `warning`, `error`, `critical`, `alert`, `emergency`	`notice`

Parameter	Meaning	Possible Values	Default Setting
Syslog server entries			
Index	Sequential number of the syslog server entry in the table. When you delete an entry, this leaves a gap in the numbering. When you create a new entry, the device fills the first gap.	1 - 8	-
IP address	Address of a syslog server to which the device sends its log entries.	Valid IPv4 address	0.0.0.0
Port	UDP port at which your syslog server receives entries.	1 - 65.535	514
Minimum level to report	Minimum level to report for an event for the device to sent a log entry for it to this syslog server.	`debug`, `informational`, `notice`, `warning`, `error`, `critical`, `alert`, `emergency`	critical
Active	Activate or deactivate the current syslog server entry in the table.	`active` (box selected), `inactive` (box empty)	active

Table 87: Syslog server entries

Parameter	Meaning	Possible Values	Default Setting
Buttons			
“Write” button	Click on “Write” to temporarily save the data. **Note:** If you have entered an IP address different to 0.0.0.0 for a newly created syslog server entry, after the entry is written the device activates it automatically. Click on “Load” for the device to update the display.	-	
“Create” button	Creates a new syslog server entry in the list.	-	
“Delete” button	Deletes the selected syslog server entry/entries from the list.	-	

Table 88: Syslog entries, buttons

Note: When you activate the logging of SNMP requests, the device sends these as events with the preset level to report `notice` to the list of syslog servers. The preset minimum level to report for a syslog server entry is `critical`.

To send SNMP requests to a syslog server, you have a number of options to change the default settings. Select the ones that meet your requirements best.

- Set the level to report for which the device creates SNMP requests as events to `warning` or `error` and change the minimum level to report for a syslog entry for one or more syslog servers to the same value.
  You also have the option of creating a separate syslog server entry for this.
- Only set the level to report for SNMP requests to `critical` or higher. The device then sends SNMP requests as events with the level to report `critical` or higher to the syslog servers.
- Only set the minimum level to report for one or more syslog server entries to `notice` or lower. Then it may happen that the device sends a large number of events to the syslog servers.

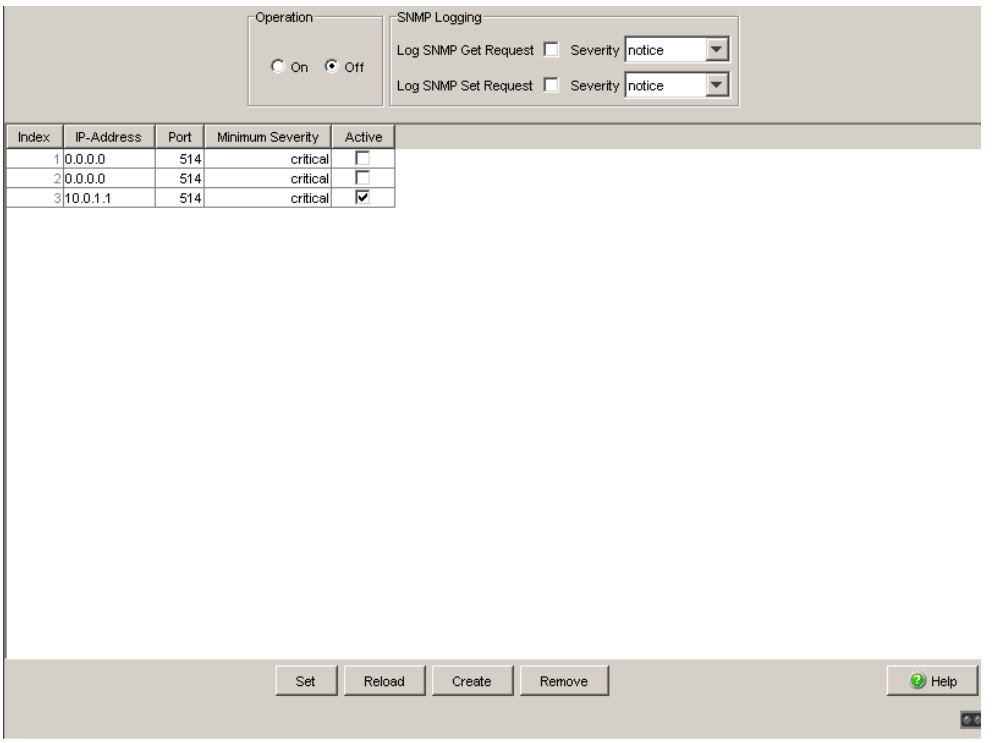


Figure 55: Syslog dialog

8.2 Event Log

The table lists the logged events with a time stamp.
The “Load” button allows you to update the content of the event log, and with the “Delete” button you delete the content of the event log.

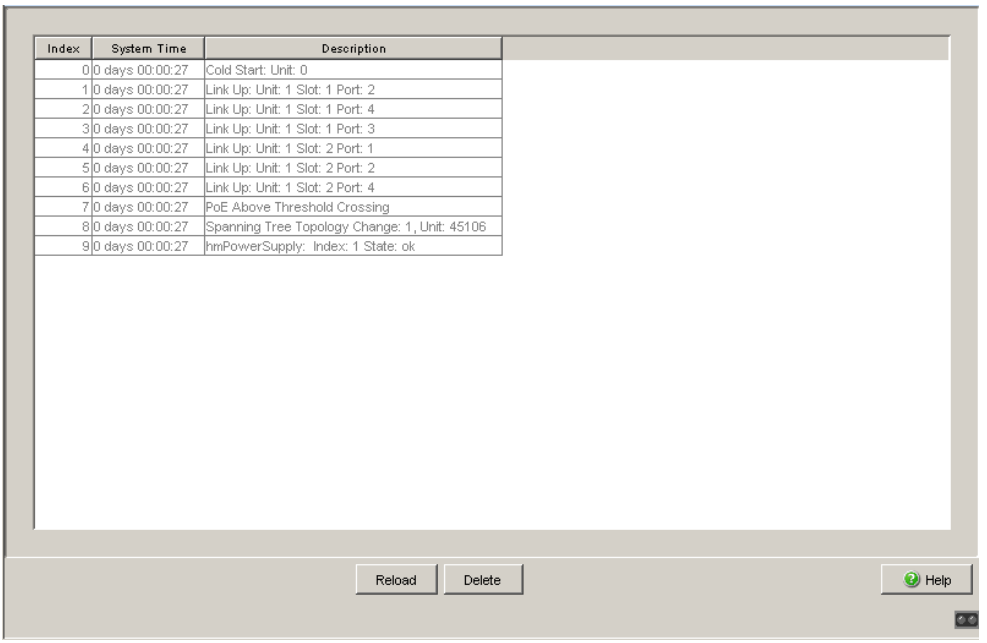

Index
System Time
Description
0 0 days 00:00:27 Cold Start: Unit: 0
1 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 2
2 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 4
3 0 days 00:00:27 Link Up: Unit: 1 Slot: 1 Port: 3
4 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 1
5 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 2
6 0 days 00:00:27 Link Up: Unit: 1 Slot: 2 Port: 4
7 0 days 00:00:27 PoE Above Threshold Crossing
8 0 days 00:00:27 Spanning Tree Topology Change: 1, Unit: 45106
9 0 days 00:00:27 hmPowerSupply: Index: 1 State: ok
Reload
Delete
Help

Figure 56: Event log table

You have the option to also send the logged events to one or more syslog servers (see on page 206 “Syslog“).

8.3 Ports

The port menu contains displays and tables for the individual ports:

- Statistics table
- Utilization
- SFP Modules
- TP cable diagnosis

8.3.1 Statistics table

This table shows you the contents of various event counters. In the Restart menu item, you can reset all the event counters to zero using "Warm start", "Cold start" or "Reset port counter".
The packet counters add up the events sent and the events received.

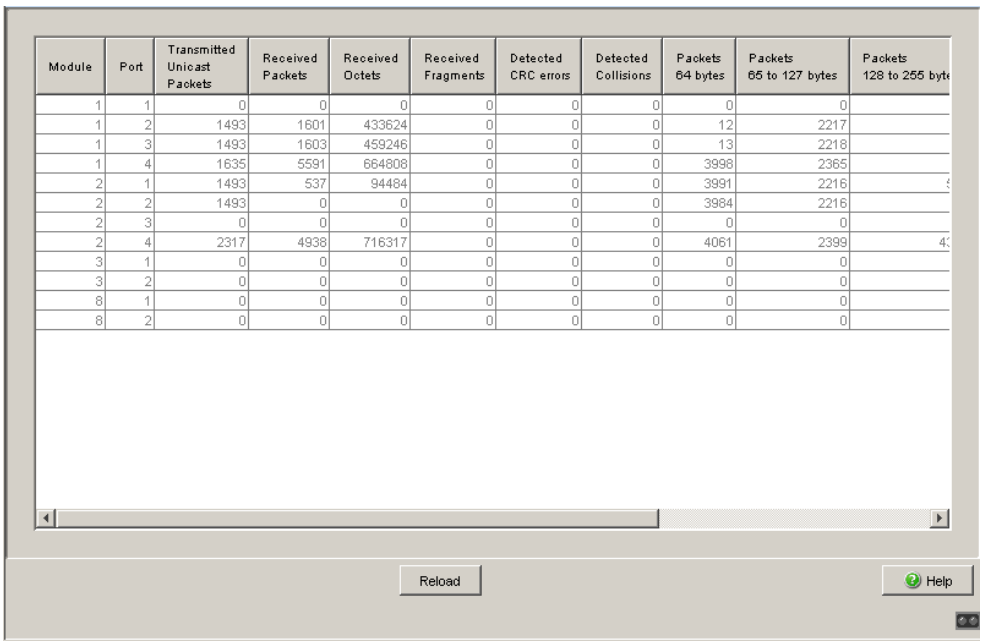


Figure 57: Port statistics table

8.3.2 Utilization

This table displays the network load of the individual ports.
In the “Upper Threshold[%]” column you enter the upper threshold value for network load. If this threshold value is exceeded, the device sets a check mark in the “Alarm” field.
In the “Lower Threshold [%]” column you enter the lower threshold value for network load. If the current load falls below this threshold value, the device removes the check mark previously set.

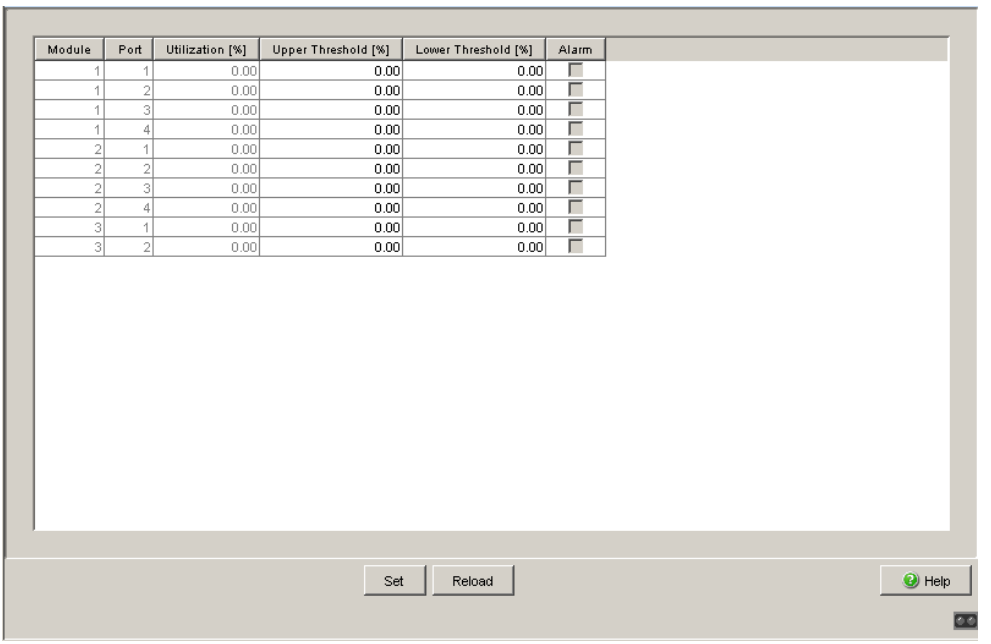


Figure 58: Network load dialog

8.3.3 SFP modules

The SFP status display allows you to look at the current SFP module connections and their properties. The properties include:

Parameter	Meaning
Module	Module of the device on which the port is located.
Port	Port to which this entry applies.
Module type	Type of SFP module, e.g. M-SFP-SX/LC
Supported	Shows whether the media module supports the SFP module.
Temperature in Celsius	Shows the operating temperature of the SFP
Tx Power in mW	Shows the transmission power in mW
Rx Power in mW	Shows the receiver power in mW
Receiver power status	Shows the power level of the received signal. – `good receiver power` – `limited receiver power` – `insufficient receiver power`

Table 89: SFP Modules dialog

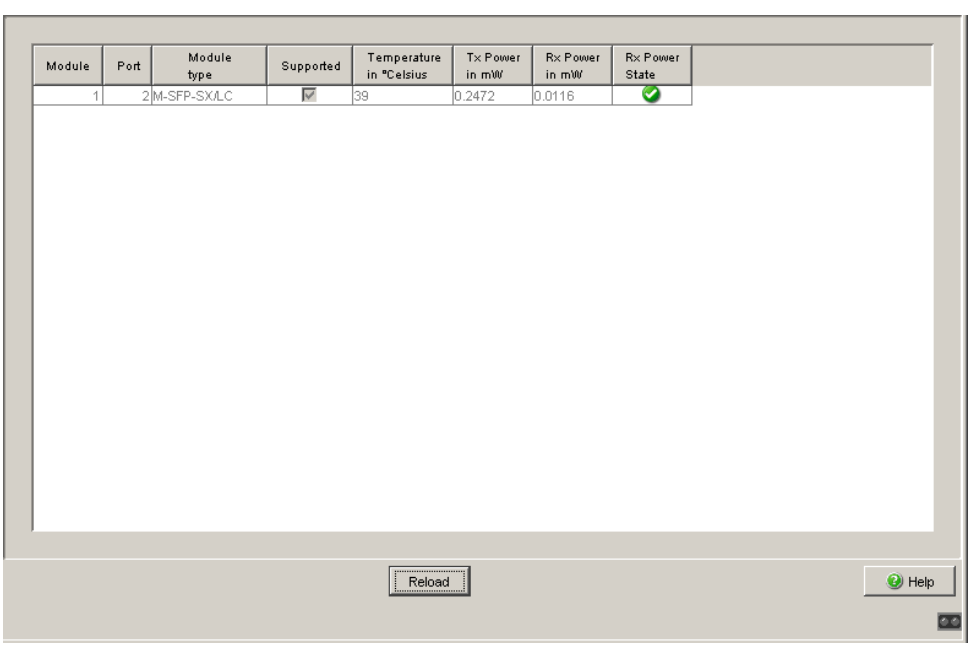


Figure 59: SFP Modules dialog

8.3.4 TP Cable Diagnosis

The TP cable diagnosis allows you to check the connected cables for short-circuits or interruptions.

Note: While the check is running, the data traffic at this port is suspended.

☐ Select the TP port on which you want to perform the check.

☐ Click "Set" to start the check.

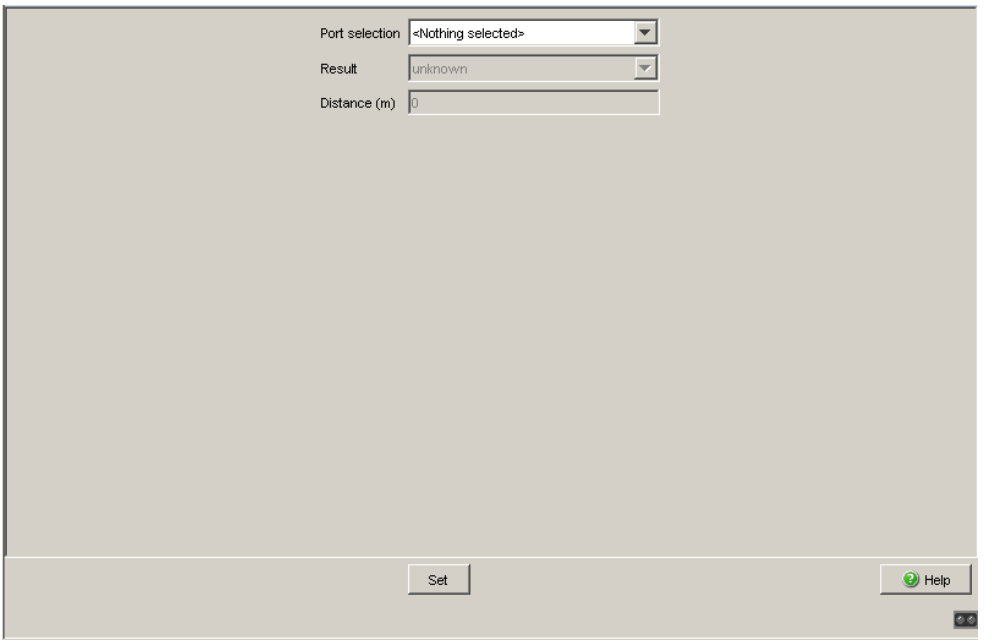


Figure 60: TP cable diagnosis dialog

The check takes a few seconds. After the check, the "Result" row contains the result of the cable diagnosis. If the result of the check shows a cable problem, then the "Distance" row contains the cable problem location's distance from the port.

Result	Meaning
normal	The cable is okay.
open	The cable is interrupted.
short circuit	There is a short-circuit in the cable.
unknown	No cable check was performed yet, or it is currently running

Table 90: Meaning of the possible results

Prerequisites for correct TP cable diagnosis:

- 1000BASE-T port, connected to a 1000BASE-T port via 8-core cable or
- 10BASE-T/100BASE-TX port, connected to a 10BASE-T/100BASE-TX port.

8.4 Configuration Check

This dialog enables you to compare the configuration for the device with the configurations of its neighbor devices.
The device includes all neighbor devices it can determine with Topology Discovery (LLDP) in the evaluation. If the configuration for the device is not compatible with the configuration for the neighbor device or somehow different, you can display detailed information on this possible configuration problem/configuration error in the dialog.

Note: If the neighbor device does not support LLDP (e.g. in the case of a hub or unmanaged switch), the dialog will show you the nearest device connected to it which is transmitting LLDP packets. If multiple devices are connected to this neighbor device without LLDP support which are transmitting LLDP packages, the device will show you each of these as a neighbor device.

Parameter	Meaning
Module	Module number for modular devices, otherwise 1.
Port	Port to which this entry applies.
Neighbour System Name	System name of the neighboring device (see on page 17 “System Data“)
Neighbour IP Address	IP address of the neighboring device with LLDP function (see on page 22 “Network“)
Neighbour Port	Displays information on the neighboring device.
Neighbour Type	Displays the type of the neighboring device. Written in – Capital letters: The device has this function, and the function is activated. – Lower-case letters: The device has this function, and the function is deactivated.
Status	Displays the configuration status – Green circle with checkmark: The configuration of this device and the configuration of the neighboring device are compatible. Communication between the two devices is okay. – Yellow warning triangle: The configuration of this device and the configuration of the neighboring device do not match. The performance of the communication between the two devices could be endangered. Select this row to obtain further information in the window below. – Red square with X: The configuration of this device and the configuration of the neighboring device are not compatible. Communication between the two devices is endangered. Select this row to obtain further information in the window below. – Blue circle with question mark: Configuration data is not available for the neighboring device. Select this row to obtain further information in the window below.
Reason	If a reason is entered in a row, selecting this row displays more detailed information on this reason in the window below.

Table 91: Configuration Check table

8.5 Topology Discovery

This dialog allows you to switch on/off the topology discovery function (LLDP). The topology table shows you the collected information for neighboring devices. This information enables the network management station to map the structure of your network.

The option "Show LLDP entries exclusively" allows you to reduce the number of table entries. In this case, the topology table hides entries from devices without active LLDP support.

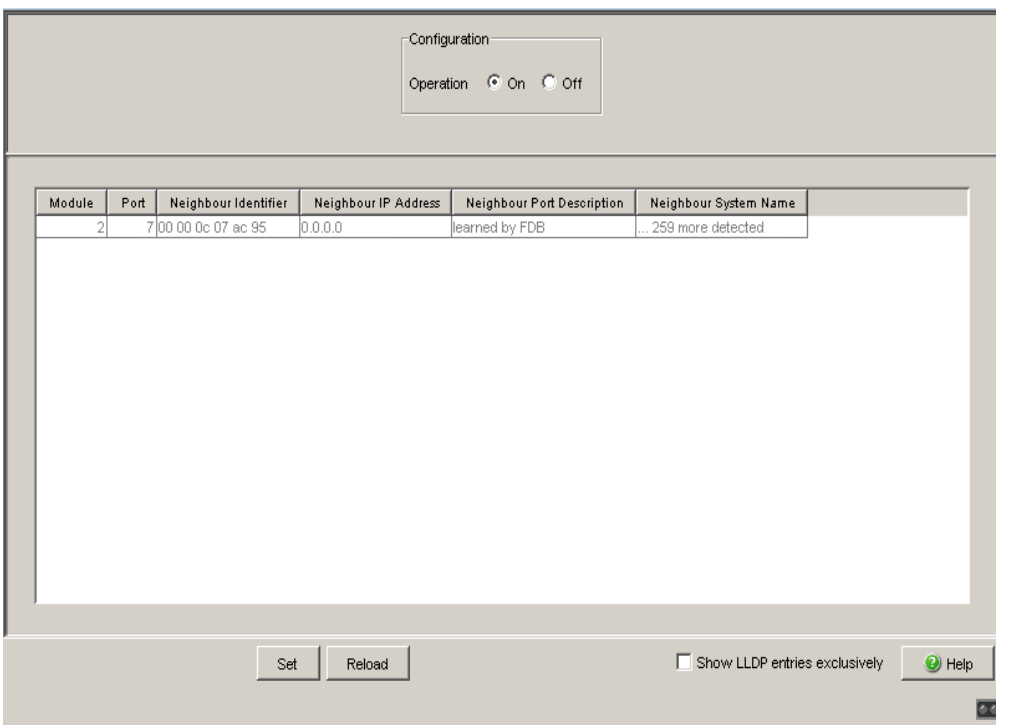


Figure 61: Topology discovery

If several devices are connected to one port, for example via a hub, the table will contain one line for each connected device.

When devices both with and without an active topology discovery function are connected to a port, the topology table hides the devices without active topology discovery.

If only devices without active topology discovery are connected to a port, the table will contain one line for this port to represent all devices. This line contains the number of connected devices
MAC addresses of devices that the topology table hides for the sake of clarity, are located in the address table (FDB), (see on page 94 “Filters for MAC addresses“).

8.6 Port Mirroring

The port mirroring function enables you to review the data traffic at up to 8 ports of the device for diagnostic purposes. The device additionally forwards (mirrors) the data for these ports to another port. This process is also called port mirroring.
The ports to be reviewed are known as source ports. The port to which the data to be reviewed is copied is called the destination port. You can only use physical ports as source or destination ports.

In port mirroring, the device copies valid incoming **and** outgoing data packets of the source port to the destination port. The device does not affect the data traffic at the source ports during port mirroring.
A management tool connected at the destination port, e.g. an RMON probe, can thus monitor the data traffic of the source ports in the sending and receiving directions.

The destination port forwards all data to be sent.
On the devices PowerMICE, MACH 104, MACH 1040 and MACH 4000, the destination port blocks received data, on all other devices, the destinations port also forwards received data.

☐ Select the source ports whose data traffic you want to review from the list of physical ports by checkmarking the relevant boxes.
You can select a maximum of 8 source ports. Ports that cannot be selected are displayed as inactive by the device, e.g. the port currently being used as the destination port, or if you have already selected 8 ports. Default setting: no source ports.

☐ Select the destination port to which you have connected your management tool from the list element in the “Destination Port” frame. The device does not display ports that cannot be selected in the list, e.g. the ports currently being used as source ports. Default setting: port 0.0 (no destination port).

☐ Select “On” in the “Function” frame to switch on the function. Default setting: “Off”.

The “Reset configuration” button in the dialog allows you to reset all the port mirroring settings of the device to the state on delivery.

Note: When port mirroring is active, the specified destination port is used solely for reviewing, and does not participate in the normal data traffic.

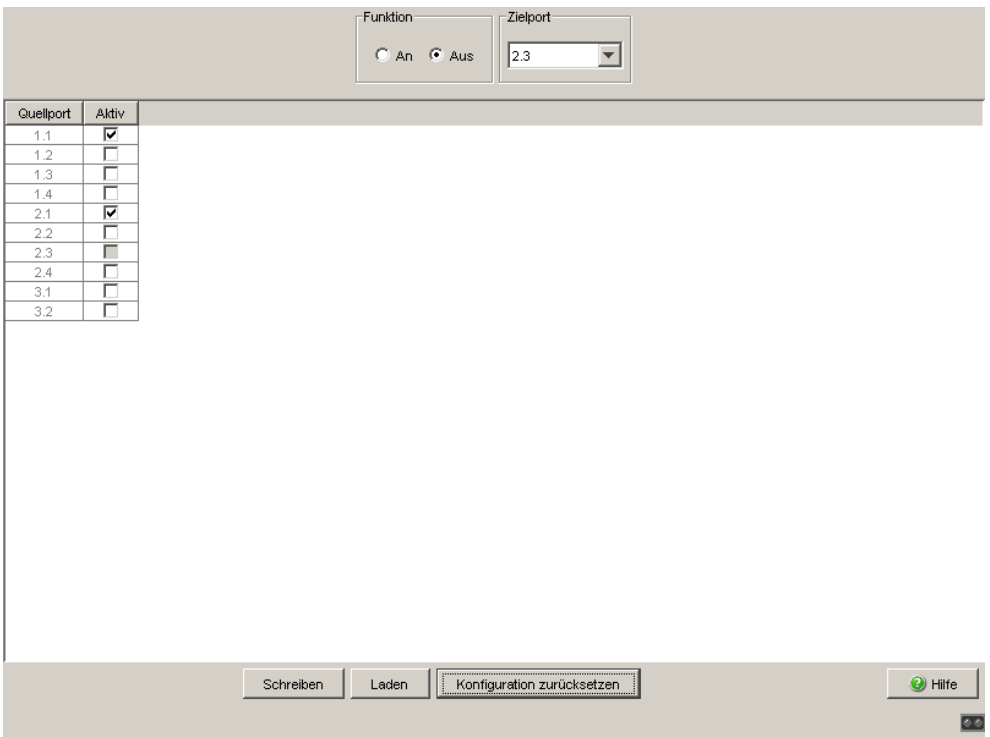


Figure 62: Port Mirroring dialog

8.7 Device Status

The device status provides an overview of the overall condition of the device. Many process visualization systems record the device status for a device in order to present its condition in graphic form.

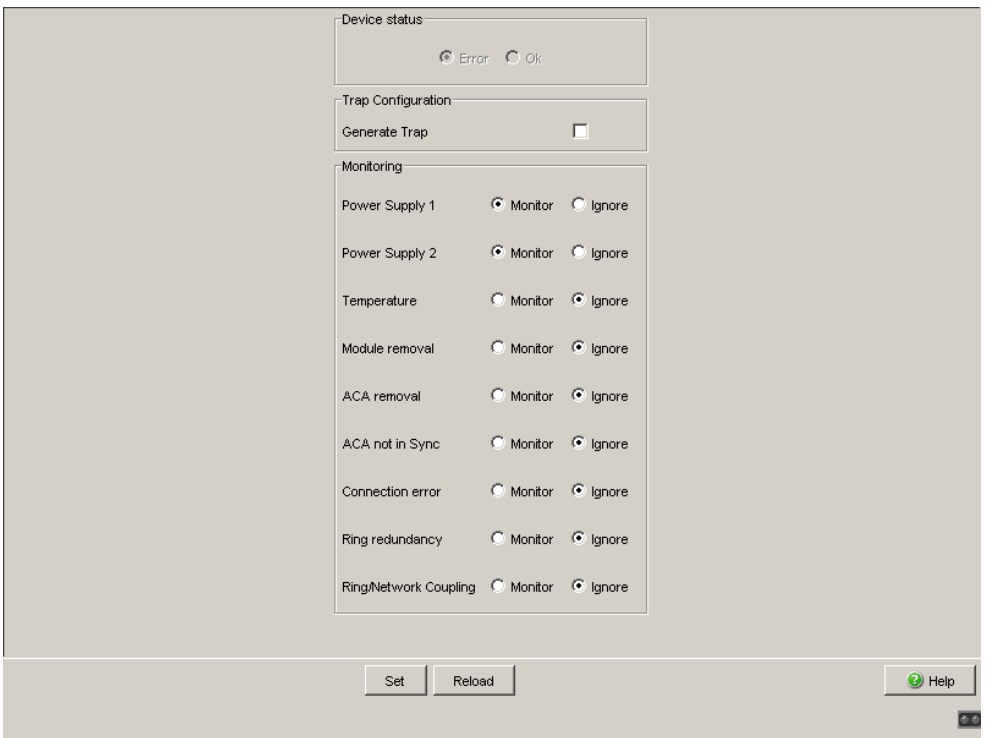


Figure 63: Device State dialog (for PowerMICE)

☐ In the "Monitoring" field, you select the events you want to monitor.
☐ To monitor the temperature, you set the temperature thresholds in the `Basics:System` dialog at the end of the system data.

The events which can be selected are:

Name	Meaning
Power supply ...	Monitor/ignore supply voltage(s).
Temperature	Monitor/ignore temperature thresholds set (see on page 16 “System“) for temperatures that are too high/too low
Module removal	Monitor/ignore the removal of a module (for modular devices).
ACA removal	Monitor/ignore the removal of the ACA.
ACA not in sync	Monitor/ignore the non-matching of the configuration in the device and on the ACA[a]
Connection error	Monitor/ignore the link status (Ok or inoperable) of at least one port. The reporting of the link status can be masked for each port by the management (see on page 27 “Port Configuration“). Link status is not monitored in the state on delivery.
Ring Redundancy	Monitor/ignore the redundancy failing (for the HIPER-Ring, only in ring manager operation). On delivery, ring redundancy is not monitored. **Note:** If the device is a normal ring member and not a ring manager, it doesn't report anything for the HIPER-Ring; for the Fast HIPER-Ring and for MRP it only reports local configuration problems.
Ring/Network coupling	Monitor/ignore the redundant coupling failing. On delivery, no monitoring of the redundant coupling is set. For two-Switch coupling with control line, the slave additionally reports the following conditions: – Incorrect link status of the control line – Partner device is also a slave (in standby mode). **Note:** In two-Switch coupling, both Switches must have found their respective partners.
Fan	Monitor/ignore fan function (for devices with fan).

Table 92: Device Status

a. The configurations are non-matching if only one file exists or the two files do not have the same content.

☐ Select "Generate Trap" in the "Trap Configuration" field to activate the sending of a trap if the device state changes.

Note: With a non-redundant voltage supply, the device reports the absence of a supply voltage. If you do not want this message to be displayed, feed the supply voltage over both inputs or switch off the monitoring (see on page 227 “Signal contact“).

8.8 Signal contact

The signal contacts are used for

- controlling external devices by manually setting the signal contacts,
- monitoring the functions of the device,
- reporting the device state of the device.

8.8.1 Manual setting

☐ Select the tab page "Alarm 1" or "Alarm 2" (for devices with two signal contacts).
☐ In the "Signal contact mode" field, you select the "Manual setting" mode. With this mode you can control this signal contact remotely.
☐ Select "Opened" in the "Manual setting" frame to open the contact.
☐ Select "Closed" in the "Manual setting" frame to close the contact.

Application options:

- Simulation of an error during SPS monitoring.
- Remote control of a device via SNMP, such as switching on a camera.

8.8.2 Function monitoring

☐ Select the tab “Signal contact 1” or “Signal contact 2” (for devices with two signal contacts).

☐ In the “Mode Signal contact” box, you select the “Monitoring correct operation” mode. In this mode, the signal contacts monitor the functions of the device, thus enabling remote diagnosis.
A break in contact is reported via the potential-free signal contact (relay contact, closed circuit).

- Loss of the supply voltage 1/2 (either of the external voltage supply or of the internal voltage).[1] Select “Monitor” for the respective power supply if the signal contact shall report the loss of the power supply voltage, or of the internal voltage that is generated from the external power supply.
- One of the temperature thresholds has been exceeded (see on page 17 “System Data“). Select “Monitor” for the temperature if the signal contact should report an impermissible temperature.
- Removing a module. Select “Monitor” for removing modules if the signal contact is to report the removal of a module (for modular devices).
- Fan inoperable (for devices with a fan).
- The removal of the ACA. Select “Monitor” for ACA removal if the signal contact is to report the removal of an ACA (for devices which support the ACA).
- Non-matching of the configuration in the device and on the ACA[2]. Select “Monitor” ACA not in sync if the signal contact is to report the non-matching of the configuration (for devices which support ACA).
- The inoperable link status of at least one port. The reporting of the link status can be masked via the management for each port in the device. Link status is not monitored in the state on delivery. Select “Monitor” for bad connections if the signal contact is to report an inoperative link status for at least one port.
- If the device is part of a redundant ring: the elimination of the reserve redundancy (i.e. the redundancy function did actually switch on), (see on page 139 “Ring Redundancy“). Select “Monitor” for the ring redundancy if the signal contact is to report the elimination of the reserve redundancy in the redundant ring.
  Default setting: no monitoring.

1. You can install additional power supplies in a MACH4000 device, which the device reports as P3-1, P3-2, P4-1 and P4-2 in its user interfaces. You will find details on the power supplies in the document Installation Guide.
2. The configurations are non-matching if only one file exists or the two files do not have the same content.

Note: If the device is a normal ring member and not a ring manager, it doesn't report anything for the HIPER-Ring; for the Fast HIPER-Ring and for MRP it only reports local configuration problems.

- The elimination of the reserve redundancy for the ring/network coupling (i.e. the redundancy function did actually switch on). Select “Monitor” for the ring/network coupling if the signal contact is to report the elimination of the reserve redundancy for the ring/network coupling (see on page 157 “Preparing a Ring/Network coupling“).
  Default setting: no monitoring.

  Note: In two-Switch coupling, both Switches must have found their respective partners.

8.8.3 Device status

☐ Select the tab page “Alarm 1” or “Alarm 2” (for devices with two signal contacts).
☐ In the “Mode Signal Contact” field, you select the “Device status” mode. In this mode, the signal contact monitors the device status (see on page 224 “Device Status“) and thereby offers remote diagnosis.
The device status “Error detected” (see on page 224 “Device Status“) is reported by means of a break in the contact via the potential-free signal contact (relay contact, closed circuit).

8.8.4 Configuring traps

☐ Select `generate Trap`, if the device is to create a trap as soon as the position of a signal contact changes when function monitoring is active.

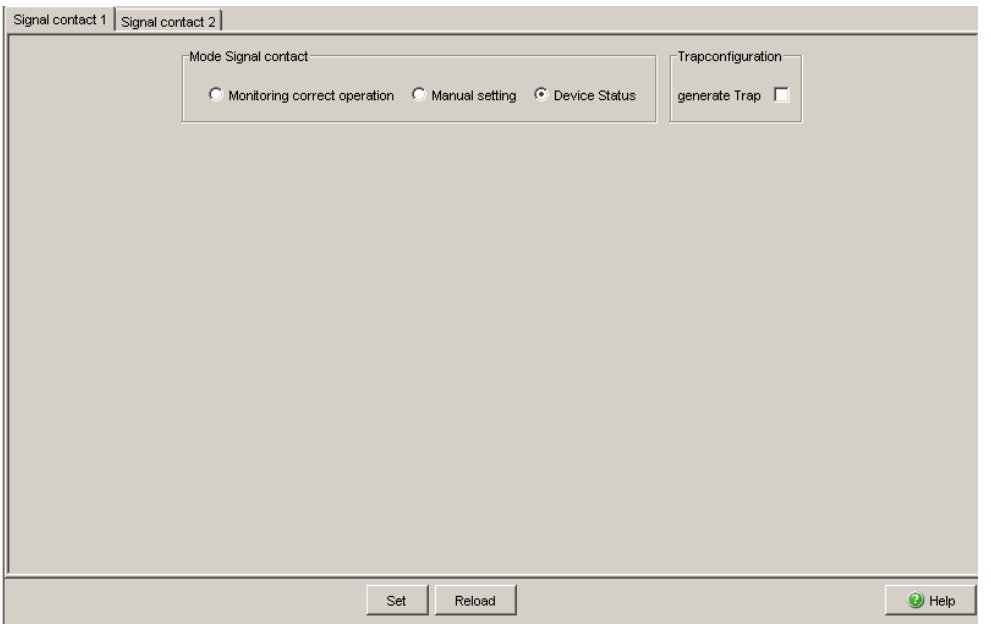


Figure 64: Signal contact dialog

8.9 Alarms (Traps)

This dialog allows you to determine which events trigger an alarm (trap) and where these alarms should be sent.

☐ Select "Create entry“.
☐ In the "Address“ column, enter the IP address of the management station to which the traps should be sent.
☐ In the "Active“ column, you mark the entries which should be taken into account when traps are sent.
☐ In the "Selection“ frame, select the trap categories from which you want to send traps.

The events which can be selected are:

Name	Meaning
Authentication	The device has rejected an unauthorized access attempt (see on page 45 “SNMPv1/v2 Access Settings“).
Link Up/Down	At one port of the device, the link to another device has been established/ interrupted.
Spanning Tree	The topology of the Rapid Spanning Tree has changed.
Chassis	Summarizes the following events: – The status of a supply voltage has changed (see the System dialog). – The status of the signal contact has changed. To take this event into account, you activate “Create trap when status changes” in the `Diagnostics:Signal Contact 1/2` dialog. – A media module has been added or removed (only for modular devices). - The AutoConfiguration Adapter(ACA), has been added or removed. - The configuration on the AutoConfiguration Adapter(ACA) does not match that in the device. – The temperature thresholds have been exceeded/not reached. – The receiver power status of a port with an SFP module has changed (see dialog `Dialog:Ports:SFP Modules`). – The configuration has been successfully saved in the device and in the AutoConfiguration Adapter(ACA), if present. – The configuration has been changed for the first time after being saved in the device.
Redundancy	The redundancy status of the ring redundancy (redundant line active/ inactive) or (for devices that support redundant ring/network coupling) the redundant ring/network coupling (redundancy exists) has changed.
Port security	On one port a data packet has been received from an unauthorized terminal device (see the `Port Security` dialog).

Table 93: Trap categories

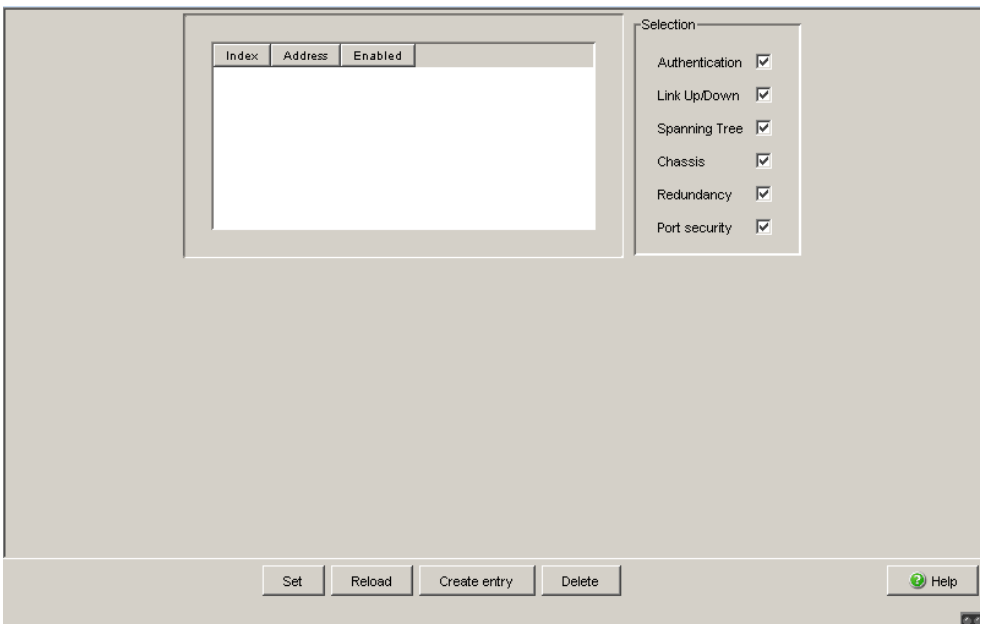


Figure 65: Alarms Dialog

8.10 Report

The following reports are available for the diagnostics:

- Log file.
  The log file is an HTML file in which the device writes important device-internal events.
- System information.
  The system information is an HTML file containing system-relevant data.

Note: You have the option to also send the logged events to one or more syslog servers (see on page 206 “Syslog“).

The following buttons are available:

- Download Switch-Dump.
  This button allows you to download system information as files in a ZIP archive (see table 94).

  ☐ Select the directory in which you want to save the switch dump.

  ☐ Click “Save”.

  The device creates the file name of the switch dumps automatically in the format <IP address>_<system name>.zip, e.g. for a device of the type PowerMICE: “10.0.1.112_PowerMICE-517A80.zip”.

- Download JAR file.
  This button allows you to download the applet of the Web-based interface as a JAR file. Then you have the option to start the applet outside of a browser.
  This facilitates the device administration even when you have disabled its web server for security reasons.

  ☐ Select the directory in which you want to save the applet.

  ☐ Click “Save”.

The device creates the file name of the applet automatically in the format <device type><software variant><software version)>_<software revision of applet>.jar, e.g. for a device of type PowerMICE with software variant L3P: “pmL3P06000_00.jar”.

File	Name	Format	Comments
Log file	event_log.html	HTML	
System information	systemInfo.html	HTML	
Event log	traplog.txt	Text	
Device configuration (binary)	switch.cfg, powermice.cfg or .mach.cfg	Binary	File name depends on device type.
Device configuration (as script)	switch.cli, powermice.cli or .mach.cli	Script	File name depends on device type.
Internal memory extract for the manufacturer to improve the product	dump.hmd	Binary	
Exception log	exception_log.html	HTML	
Output of CLI commands[a]: – show running-config[b] – show port all – show sysinfo – show mac-address-table – show mac-filter-table igmpsnooping	clicommands.txt	Text	

Table 94: Files in switch dump archive

a: Prerequisite: a Telnet connection is available.

b: Prerequisite: you are logged in as a user with write access.

8.11 IP address conflict detection

This dialog allows you to detect address conflicts the device is having with its own IP address and rectify them (Address Conflict Detection, ACD).

☐ Select IP address conflict detection on/off under “Status” or select the mode (see table 95).

Mode	Meaning
enable	Enables active and passive detection.
disable	Disables the function
activeDetectionOnly	Enables active detection only. After connecting to a network or after an IP address has been configured, the device immediately checks whether its IP address already exists within the network. If the IP address already exists, the device will return to the previous configuration, if possible, and make another attempt after 15 seconds. This prevents the device from connecting to the network with a duplicate IP address.
passiveOnly	Enables passive detection only. The device listens passively on the network to determine whether its IP address already exists. If it detects a duplicate IP address, it will initially defend its address by employing the ACD mechanism and sending out gratuitous ARPs. If the remote device does not disconnect from the network, the management interface of the local device will then disconnect from the network. Every 15 seconds, it will poll the network to determine if there is still an address conflict. If there isn't, it will connect back to the network.

Table 95: Possible address conflict operation modes

▶ In the table the device logs IP address conflicts with its IP address.
For each conflict the device logs:
  ▶ the time
  ▶ the conflicting IP address
  ▶ the MAC address of the device with which the IP address conflicted.

For each IP address, the device logs a line with the last conflict that occurred.

☐ You can delete this table by restarting the device.

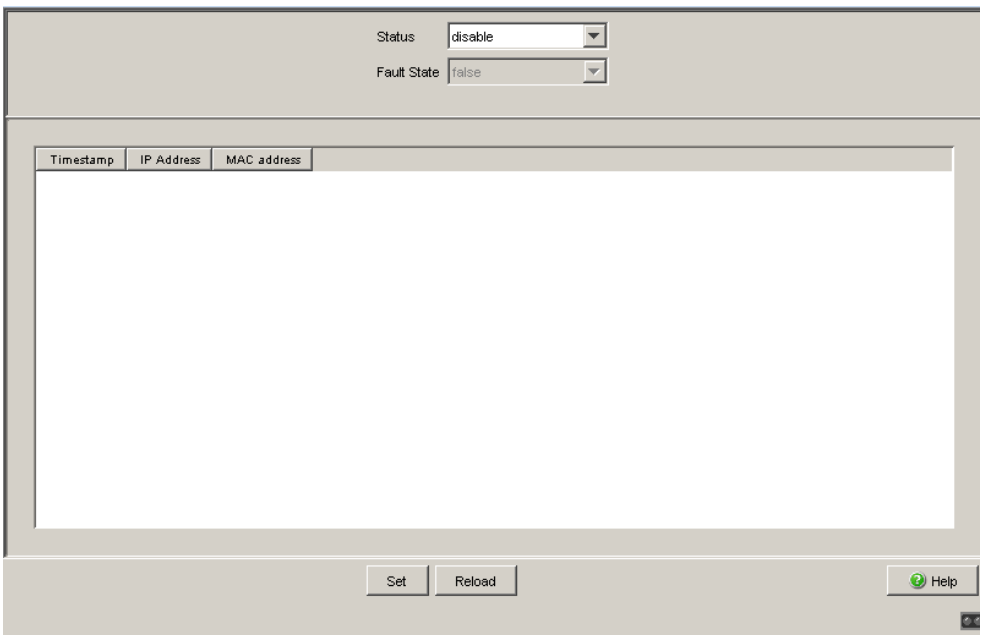


Figure 66: IP Address Conflict Detection dialog

8.12 Self Test

With this dialog you can:

- activate/deactivate the RAM test for a cold start of the device. Deactivating the RAM test cuts the booting time for a cold start of the device.
- allow or disable a restart due to an undefined software or hardware state.

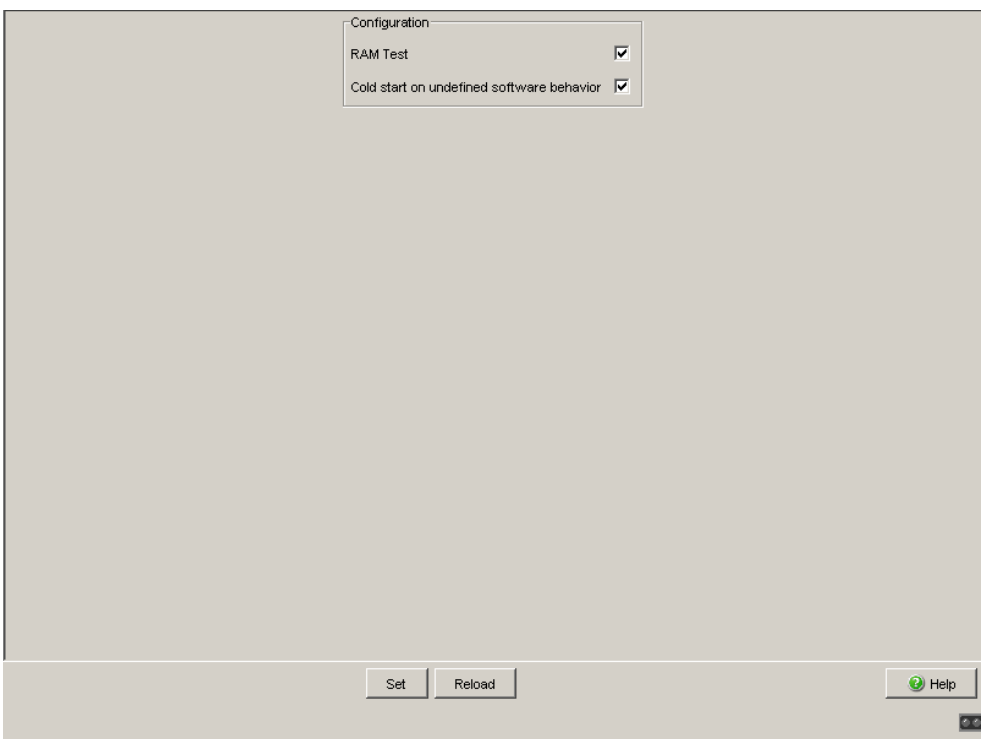


Figure 67: Self-test dialog

8.13 Service mode

The following devices support the service mode:
RS20/RS30/RS40 and MS20/MS30.

The service mode enables you to divide the device into 2 transmission areas. You can thus, for example, perform test or service configurations in the field area of a network while the ongoing operation continues in the backbone area.

The device specifies the two transmission areas via the HIPER-Ring ports: transmission area 1 only includes the HIPER-Ring ports of the device, while all other ports belong to transmission area 2. When the service mode is activated, the device creates a new VLAN in which all the ports of transmission area 2 are members. You use the redundant supply voltage (see below) to activate the service mode. You can view the configuration of the newly created VLAN in the dialogs under Switching/VLAN, but the device does not allow these entries to be changed, in order to keep the service configuration.
By generating the VLAN, the device

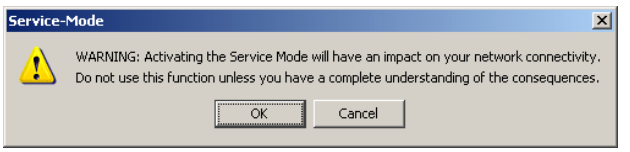
- resets the port VLAN IDs for all the ports of this VLAN to the new VLAN ID
- deactivates GVRP at all ports of this VLAN. The device thus prevents GVRP from dynamically changing the service mode port settings.
- activates “ingress filtering” at all ports of this VLAN. Thus the device only transmits packets when the input and output ports belong to this VLAN.

8.13.1 Activating the service mode

Prerequisites:
– HIPER-Ring ports are defined (HIPER-Ring or MRP-Ring).
– The supply voltage is redundant at P1 and P2.

Note: If there is no redundant voltage when activating the service mode (by clicking on “Set” - see below), the switch immediately creates the 2 switching areas. Depending on the settings already entered, this may interrupt your communication to the switch.

☐ Select the `Diagnostics:Service Mode` dialog.
☐ Activate “Mode”.
☐ Enter a number other than 0 or 1 in the “VLAN” field. Enter a VLAN ID for a new VLAN in order to keep the settings for existing VLANs.
☐ Click “Set”. The device outputs the following system message:


Service-Mode
WARNING: Activating the Service Mode will have an impact on your network connectivity.
Do not use this function unless you have a complete understanding of the consequences.
OK
Cancel

☐ If you have verified that your communication with the Switch will not be interrupted, click “OK” to activate the service mode.

The device will indicate in all dialogs that the service mode is activated.

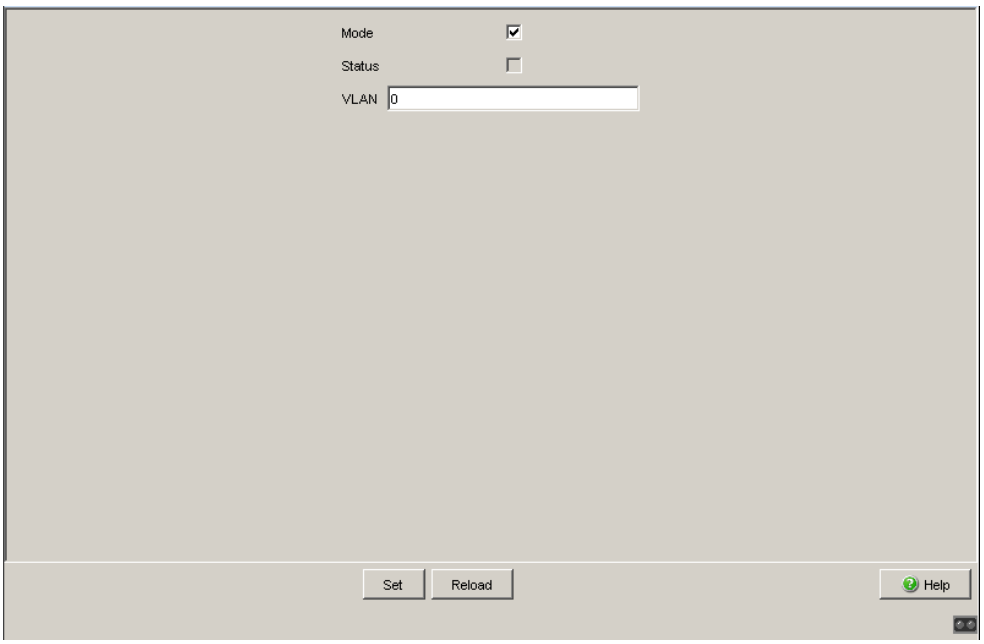


Figure 68: Service Mode dialog - mode activated

☐ Deactivate the redundant supply voltage.

The service mode is now activated, which the device indicates with a checkmark in the “Status” field.

Note: Deactivate the service mode (see below) when saving the device configuration (dialog: `Basics:Load/Save:Save:On the Switch`).

8.13.2 Deactivating the service mode

☐ Reactivate the redundant voltage.

The service mode is now deactivated.

☐ Select the `Diagnostics:Service Mode` dialog.

☐ Deactivate “Mode”.
☐ Click “Set” to deactivate the service mode so that the device will no longer switch to the service mode if the redundant voltage supply is lost.

Note: After the service mode is deactivated, the device takes on its previous settings again.

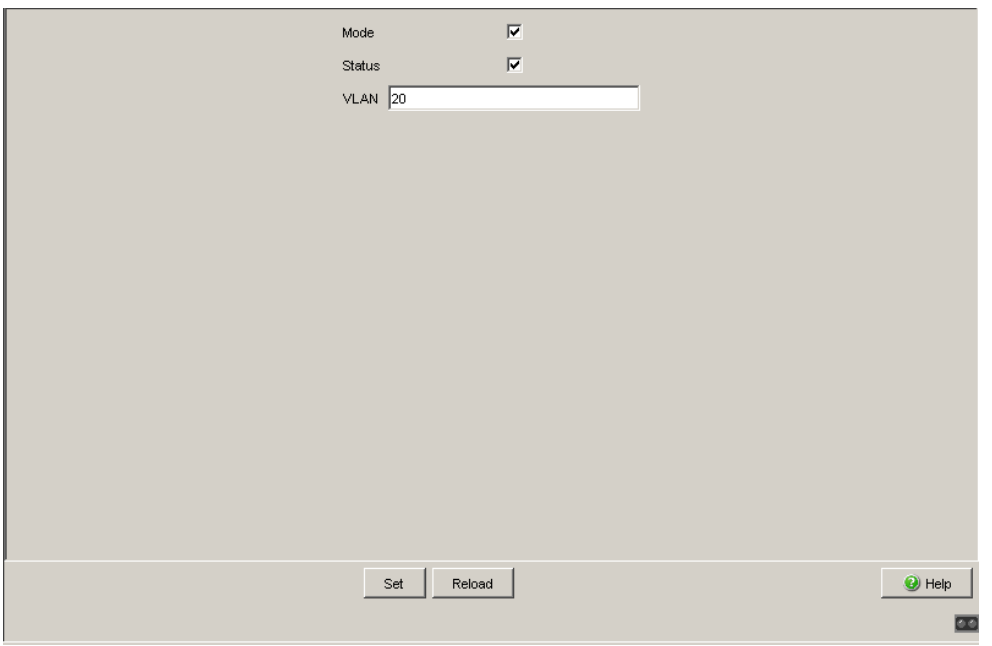


Figure 69: Service Mode dialog - mode deactivated

A Appendix

A.1 Technical Data

Switching	
Size of MAC address table (incl. static filters)	8,000 (16,000 for PowerMICE and MACH 4000)
Max. number of statically configured MAC address filters	100
Max. number of MAC address filters learnable via GMRP/IGMP Snooping	512 (RS20/RS30/RS40, RSR20/RSR30, MS20/ MS30, OCTOPUS, MACH 100, MACH 1000) 1.000 (PowerMICE, MACH 104, MACH 1040, MACH 4000)
Max. length of over-long packets (from rel. 03.0.00)	1,632 bytes (RS20/RS30/RS40, RSR20/RSR30, MS20/ MS30, OCTOPUS, MACH 100, MACH 1000) 1,552 bytes (PowerMICE, MACH 104, MACH 1040, MACH 4000)

VLAN	
VLAN ID	1 to 4,042 (MACH 4000: 3,966)
Number of VLANs	max. 255 simultaneously per device (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per device) max. 255 simultaneously per port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per port)
Number of VLANs in GMRP in VLAN 1	max. 255 simultaneously per device (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per device) max. 255 simultaneously per port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 simultaneously per port)

A.2 List of RFCs

RFC 768	(UDP)
RFC 783	(TFTP)
RFC 791	(IP)
RFC 792	(ICMP)
RFC 793	(TCP)
RFC 826	(ARP)
RFC 854	(Telnet)
RFC 855	(Telnet Option)
RFC 951	(BOOTP)
RFC 1112	(IGMPv1)
RFC 1157	(SNMPv1)
RFC 1155	(SMIv1)
RFC 1212	(Concise MIB Definitions)
RFC 1213	(MIB2)
RFC 1493	(Dot1d)
RFC 1542	(BOOTP-Extensions)
RFC 1643	(Ethernet-like -MIB)
RFC 1757	(RMON)
RFC 1769	(SNTP)
RFC 1867	(Form-Based File Upload in HTML)
RFC 1901	(Community based SNMP v2)
RFC 1905	(Protocol Operations for SNMP v2)
RFC 1906	(Transport Mappings for SNMP v2)
RFC 1907	(Management Information Base for SNMP v2)
RFC 1908	(Coexistence between SNMP v1 and SNMP v2)
RFC 1945	(HTTP/1.0)
RFC 2068	(HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
RFC 2131	(DHCP)
RFC 2132	(DHCP-Options)
RFC 2233	(The Interfaces Group MIB using SMI v2)
RFC 2236	(IGMPv2)
RFC 2246	(The TLS Protocol, Version 1.0)
RFC 2271	(SNMP Framework MIB)
RFC 2346	(AES Ciphersuites for Transport Layer Security)
RFC 2365	(Administratively Scoped Boundaries)
RFC 2570	(Introduction to SNMP v3)
RFC 2571	(Architecture for Describing SNMP Management Frameworks)
RFC 2572	(Message Processing and Dispatching for SNMP)
RFC 2573	(SNMP v3 Applications)

RFC 2574	(User Based Security Model for SNMP v3)
RFC 2575	(View Based Access Control Model for SNMP)
RFC 2576	(Coexistence between SNMP v1, v2 & v3)
RFC 2578	(SMI v2)
RFC 2579	(Textual Conventions for SMI v2)
RFC 2580	(Conformance statements for SMI v2)
RFC 2613	(SMON)
RFC 2618	(RADIUS Authentication Client MIB)
RFC 2620	(RADIUS Accounting MIB)
RFC 2674	(Dot1p/Q)
RFC 2818	(HTTP over TLS)
RFC 2851	(Internet Addresses MIB)
RFC 2865	(RADIUS Client)
RFC 2866	(RADIUS Accounting)
RFC 2868	(RADIUS Attributes for Tunnel Protocol Support)
RFC 2869	(RADIUS Extensions)
RFC 2869bis	(RADIUS support for EAP)
RFC 2933	(IGMP MIB)
RFC 3164	(The BSD Syslog Protocol)
RFC 3376	(IGMPv3)
RFC 3580	(802.1X RADIUS Usage Guidelines)
RFC 4188	(Definitions of Managed Objects for Bridges)

A.3 Underlying IEEE Standards

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1af	Power over Ethernet
IEEE 802.1D	Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP, Spanning Tree)
IEEE 802.1Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port-Based VLANs, GVRP)
IEEE 802.1w-2001	Rapid Reconfiguration (RSTP)
IEEE 802.1X	Port Authentication
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3ad	Link Aggregation with Static LAG and LACP Support
IEEE 802.3x	Flow Control

A.4 Underlying IEC Norms

IEC 62439	High availability automation networks; especially: Chap. 5, MRP – Media Redundancy Protocol based on a ring topology

A.5 Copyright of Integrated Software

A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.5.2 Broadcom Corporation

(c) Copyright 1999-2007 Broadcom Corporation. All Rights Reserved.

B Readers' Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- by mail to

Hirschmann Automation and Control GmbH
Department AED
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Index

8
802.1x 57

A
ACA 32, 232, 232, 232
Accept SNTP Broadcast 70
Acceptable Frame Types 118
Access with Web-based interface, password 42
ACD 236
Address Conflict Detection 236
Advanced 189
AF 133
Aging Time 90
Alarm 231
Assured Forwarding 133
Auto Configuration Adapter, 232
AutoConfiguration Adapter 232

B
BPDU Guard 170
Broadcast Limiter Settings 97, 99

C
Cable crossing 27
Class Selector 133
CLI 203
CLI access, password 42
Clock 73
Cold start (after software update) 25
Coldstart 38
Command Line Interface 203
Configuration Check 218
Configuring Fast HIPER-Ring 148
Configuring the HIPER-Ring 141
Configuring the MRP-Ring 145
Configuring the Sub-Ring 151
Current VLAN dialog 113

D
Device status 224
DHCP Option 82 190
DHCP Relay Agent 190
DHCP relay agent 190
DHCP Server (global) 192
DHCP server (lease table) 198
DHCP Server (overview) 192
DHCP server pool 194
Diagnose 205
Differentiated management access 51
DiffServ 121
DIP switch 141
DSCP 121

E
EF 133
EtherNet/IP 202
Event log 211
Expedited Forwarding 133

F
FAQ 257
Fast HIPER-Ring (port VLAN ID) 118
Fast HIPER-Ring, Configuration 148
Filters for MAC addresses 94
Firmware update 24
Forward Delay 169, 171

G
General 15
Grandmaster 81

H
Hello Time 168, 171
HIPER-Ring 117, 173
HIPER-Ring (source for alarms) 232
HiVision 7

I
IEEE 802.1x 57
IGMP Querier 101
IGMP settings 101
IGMP Snooping 101
Independent VLAN 112
Industry Protocols 200
Industry protocols 7
Ingress Filtering 118
IP DSCP mapping 121, 132
IP-DSCP value 122

J
Java 11
Java Runtime Environment 11
JavaScript 11

L
LACP Link Aggregation Control Protocol 136
Link Aggregation 135, 136, 138

Link Aggregation dialog 137
Link State (Port) 27
LLDP 218, 220
Login 12

M
Max Age 169, 171
Media module (for modular devices) 232
MRP Domain 154, 155
MSTP 164
Multicasts 100
Multiple Spanning Tree 164

N
Network Management Software 7
NTP 69

O
One-Switch coupling 159
Option 82 190

P
Password 12, 44
Password for access with Web-based interface 42
Password for CLI access 42
Password for SNMPv3 access 42
Per-Hop-Behavior (PHB) 132
Port configuration 27, 125
Port configuration (QoS/priority) 125
Port Mirroring 222
Port priority 125, 127
Port Security (802.1X-based) 57
Port security (IP-/MAC-based) 54
Port security (source for alarms) 55
Port State (Link) 27
Port Statistics 212
Port VLAN ID 118
Ports 212
Power over ETHERNET 29
Precedence 133
Precision Time Protocol 73
Priority queue 122
PROFINET IO 7, 200
PROFINET IO (DCP mode per port) 201
PROFINET IO; PHY Fast Startup per Port 201
PTP 73

Q
QoS/Priority 121

R
RAM test 238
Rapid Spanning Tree 164
Rapid Spanning Tree Port Protocol 179
Rate Limiter 96
Rate Limiter Settings 97, 99
Read access 12
Reboot 38
Receiver power status 232
Redundancy functions 135
Redundancy Manager 139
Redundant 139, 164
Redundant coupling 117, 117, 135, 136, 173, 225
Reference clock 81
Report 234
Request interval (SNTP) 70, 70
Restart 38
Restore default settings 32
Restore state on delivery 32
RFC 245
Ring 139
Ring Manager 139
Ring Redundancy 135
Ring Redundancy basic configuration 140
Ring structure 139
Ring/Network Coupling 157
Ring/Network coupling 117, 135, 225
Ring/Network coupling (source for alarms) 232
Ringport 141
RMON probe 222
Root bridge 165
RSTP 164

S
Security 41
Self-test 238
Service Mode 239
Set 13
SFP Module (source for alarms) 232
SFP Modules 215
SFP status display 215
Shared VLAN 112
Signal contact 227
Signal contact (source for alarm) 232
SNMP logging 206
SNMPv1/v2 access settings 45
SNMPv3 access, password 42
SNTP 69
SNTP Broadcasts 70
SNTP client 69
SNTP server 69
Software update 24
Spanning Tree 164
SSH Access 48

Statistics table 212
STP 164
Sub-Ring - New Entry dialog 155
Sub-Ring configuration 152
Supply voltage 232
Switching 89
Switching Global Dialog 90
Symbol 9
Syslog 206
System time 70

T
Technical questions 257
Telnet Access 48
Temperature (device) 17
Temperature (SFPs) 215
Time 67
Time management 73
Timestamp unit 73
Topology 220
Topology Discovery 218
ToS 121
TP cable diagnosis 216
Training courses 257
Trap 231
Trunk 136
Trust mode 125, 128
Trustdot1p 128
TrustIpDscp 123, 129
Two-switch coupling 159
Two-Switch coupling with control line 159
TX Hold Count 169
Type of Service 121

t
trustDot1p (global trust mode) 123
trustIpDscp (global trust mode) 123, 129

U
Universal Time Coordinated 69
Untrusted 128
Untrusted (global trust mode) 122
Untrusted traffic class 125, 129
UTC 69

V
VLAN 110
VLAN (HIPER-Ring settings) 143
VLAN and GOOSE Protocol 111
VLAN and GVRP 111, 118
VLAN and redundancy rings 119
VLAN Global dialog 110
VLAN ID (network parameter of the device) 22
VLAN Mapping 121
VLAN mapping 130
VLAN mode 112
VLAN Port dialog 117
VLAN priority 121
VLAN priority 122
VLAN Static dialog 115

W
Web Access 48
Web-based interface 11
Web-based management 11
Website 12
Write access 12

D Further Support

Technical Questions and Training Courses

In the event of technical queries, please contact your local Hirschmann distributor or Hirschmann office.
You can find the addresses of our distributors on the Internet: www.hirschmann-ac.com.

Our support line is also at your disposal:

- Tel. +49 1805 14-1538
- Fax +49 7127 14-1551

Answers to Frequently Asked Questions can be found on the Hirschmann internet site (www.hirschmann-ac.com) at the end of the product sites in the FAQ category.
The current training courses to technology and products can be found under http://www.hicomcenter.com.

Hirschmann Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planing.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com.

HIRSCHMANN

A BELDEN BRAND